

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP05/002514

International filing date: 10 February 2005 (10.02.2005)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2004-033352
Filing date: 10 February 2004 (10.02.2004)

Date of receipt at the International Bureau: 31 March 2005 (31.03.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)



World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

10. 2. 2005

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 4 年 2 月 1 0 日
Date of Application:

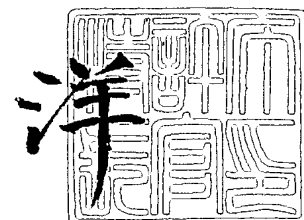
出 願 番 号 特 願 2 0 0 4 - 0 3 3 3 5 2
Application Number:
[ST. 10/C]: [J P 2 0 0 4 - 0 3 3 3 5 2]

出 願 人 エヌ・ティ・ティ・コミュニケーションズ株式会社
Applicant(s):

2 0 0 5 年 3 月 1 7 日

特許庁長官
Commissioner,
Japan Patent Office

小 川





【書類名】 特許願
【整理番号】 GLN-00469
【提出日】 平成16年 2月10日
【あて先】 特許庁長官殿
【国際特許分類】 G09C 1/00
【発明者】
 【住所又は居所】 東京都千代田区内幸町一丁目 1 番 6 号 エヌ・ティ・ティ・コ
 ミュニケーションズ株式会社内
 【氏名】 加賀谷 誠
【発明者】
 【住所又は居所】 東京都千代田区内幸町一丁目 1 番 6 号 エヌ・ティ・ティ・コ
 ミュニケーションズ株式会社内
 【氏名】 荻原 利彦
【発明者】
 【住所又は居所】 東京都千代田区内幸町一丁目 1 番 6 号 エヌ・ティ・ティ・コ
 ミュニケーションズ株式会社内
 【氏名】 野村 進
【特許出願人】
 【識別番号】 399035766
 【氏名又は名称】 エヌ・ティ・ティ・コミュニケーションズ株式会社
【代理人】
 【識別番号】 100083806
 【弁理士】
 【氏名又は名称】 三好 秀和
 【電話番号】 03-3504-3075
【選任した代理人】
 【識別番号】 100068342
 【弁理士】
 【氏名又は名称】 三好 保男
【選任した代理人】
 【識別番号】 100095500
 【弁理士】
 【氏名又は名称】 伊藤 正和
【選任した代理人】
 【識別番号】 100101247
 【弁理士】
 【氏名又は名称】 高橋 俊一
【選任した代理人】
 【識別番号】 100098327
 【弁理士】
 【氏名又は名称】 高松 俊雄
【手数料の表示】
 【予納台帳番号】 001982
 【納付金額】 21,000円
【提出物件の目録】
 【物件名】 特許請求の範囲 1
 【物件名】 明細書 1
 【物件名】 図面 1
 【物件名】 要約書 1
 【包括委任状番号】 9908855

【書類名】 特許請求の範囲**【請求項 1】**

利用者の機密情報を秘密分散法を用いて管理する機密情報管理システムであって、前記秘密分散法は、

前記機密情報を所望の処理単位ビット長に基づいて所望の分割数の分割データに分割するデータ分割方法であり、前記機密情報を処理単位ビット長毎に区分けして、複数の元部分データを生成し、この複数の元部分データの各々に対応して、前記機密情報のビット長と同じまたはこれより短い長さの乱数から処理単位ビット長の複数の乱数部分データを生成し、各分割データを構成する各分割部分データを元部分データと乱数部分データの排他的論理和によって処理単位ビット長毎に生成して、所望の分割数の分割データを生成するとともに、

新たに発生させた乱数から処理単位ビット長の複数の乱数部分データを生成し、前記各分割部分データと該乱数部分データの排他的論理和により処理単位ビット長毎に再分割部分データを生成して、前記所望の分割数の再分割データを生成するデータ分割方法であり、

前記機密情報を前記秘密分散法を用いて複数の分割データに分割するデータ分割手段と

前記複数の分割データの一部を、前記利用者が保持するための分割データとして第 1 の記憶部に記憶させるとともに、前記複数の分割データの残りを、1 又は複数の第 2 の記憶部それぞれに記憶させるデータ記憶手段と、

必要に応じて前記秘密分散法を用いて、前記第 2 の記憶部に記憶された各分割データのうち、復元可能な所定の個数の分割データの組み合わせから、複数の再分割データを作成するデータ再分割手段と、

前記複数の再分割データの一部を新たな分割データとして前記第 1 の記憶部に記憶させるとともに、前記第 2 の記憶部に記憶された各分割データを無効にして、前記複数の再分割データの残りを新たな分割データとして前記第 2 の記憶部それぞれに記憶させるデータ再記憶手段と、

を有することを特徴とする機密情報管理システム。

【請求項 2】

前記機密情報を使用する場合には、前記利用者が保持する分割データを取得し、該分割データと前記第 2 の記憶部に記憶された各分割データのうち前記所定の個数の分割データの組み合わせから前記秘密分散法を用いて前記機密情報を復元するデータ復元手段を有することを特徴とする請求項 1 記載の機密情報管理システム。

【請求項 3】

前記機密情報を使用するときは、使用した事実を使用履歴情報として記憶する使用履歴記憶手段を有することを特徴とする請求項 2 記載の機密情報管理システム。

【請求項 4】

前記機密情報を使用する場合には、前記第 2 の記憶部に記憶された各分割データのうち、前記所定の個数から前記利用者が保持する分割データの個数を引いた個数の分割データの組み合わせを前記利用者が有する端末に通信ネットワークを介して送信する分割データ送信手段を有することを特徴とする請求項 1 記載の機密情報管理システム。

【請求項 5】

前記データ再分割手段は、前記所定の個数の分割データの組み合わせに含まれる各分割データを構成するそれぞれの分割部分データ同士の排他的論理和演算によって、前記利用者が保持した分割データを生成することを特徴とする請求項 1 乃至 4 のいずれか 1 項に記載の機密情報管理システム。

【請求項 6】

前記秘密分散法は、前記各分割部分データと、該各分割部分データを生成する際に用いたそれぞれの乱数部分データに対応する新たな乱数部分データそれぞれとの排他的論理和演算により、各再分割部分データを生成することを特徴とする請求項 1 乃至 5 のいずれか

1 項に記載の機密情報管理システム。

【請求項 7】

前記秘密分散法は、さらに、前記各再分割部分データと、該各再分割部分データ生成前の各分割部分データを生成する際に用いた古い乱数部分データそれぞれの排他的論理和演算により、前記再分割部分データから古い乱数部分データを消去することを特徴とする請求項 6 記載の機密情報管理システム。

【請求項 8】

前記第 1 の記憶部に記憶される分割データを通信ネットワークを介して前記利用者が有する端末に送信する送信手段を有することを特徴とする請求項 1 乃至 7 のいずれか 1 項に記載の機密情報管理システム。

【請求項 9】

前記機密情報を前記利用者が有する端末から通信ネットワークを介して受信する受信手段を有することを特徴とする請求項 1 乃至 8 のいずれか 1 項に記載の機密情報管理システム。

【請求項 10】

利用者の機密情報を秘密分散法を用いて管理する機密情報管理方法であって、
前記秘密分散法は、

前記機密情報を所望の処理単位ビット長に基づいて所望の分割数の分割データに分割するデータ分割方法であり、前記機密情報を処理単位ビット長毎に区分けして、複数の元部分データを生成し、この複数の元部分データの各々に対応して、前記機密情報のビット長と同じまたはこれより短い長さの乱数から処理単位ビット長の複数の乱数部分データを生成し、各分割データを構成する各分割部分データを元部分データと乱数部分データの排他的論理和によって処理単位ビット長毎に生成して、所望の分割数の分割データを生成するとともに、

新たに発生させた乱数から処理単位ビット長の複数の乱数部分データを生成し、前記各分割部分データと該乱数部分データの排他的論理和により処理単位ビット長毎に再分割部分データを生成して、前記所望の分割数の再分割データを生成するデータ分割方法であり、

前記機密情報を前記秘密分散法を用いて複数の分割データに分割するデータ分割ステップと、

前記複数の分割データの一部を、前記利用者が保持するための分割データとして第 1 の記憶部に記憶させるとともに、前記複数の分割データの残りを、1 又は複数の第 2 の記憶部それぞれに記憶させるデータ記憶ステップと、

必要に応じて前記秘密分散法を用いて、前記第 2 の記憶部に記憶された各分割データのうち、復元可能な所定の個数の分割データの組み合わせから、複数の再分割データを作成するデータ再分割ステップと、

前記複数の再分割データの一部を新たな分割データとして前記第 1 の記憶部に記憶させるとともに、前記第 2 の記憶部に記憶された各分割データを無効にして、前記複数の再分割データの残りを新たな分割データとして前記第 2 の記憶部それぞれに記憶させるデータ再記憶ステップと、

を有することを特徴とする機密情報管理方法。

【請求項 11】

利用者の機密情報を秘密分散法を用いて管理するためのコンピュータが読み取り可能な機密情報管理プログラムであって、

前記秘密分散法は、

前記機密情報を所望の処理単位ビット長に基づいて所望の分割数の分割データに分割するデータ分割方法であり、前記機密情報を処理単位ビット長毎に区分けして、複数の元部分データを生成し、この複数の元部分データの各々に対応して、前記機密情報のビット長と同じまたはこれより短い長さの乱数から処理単位ビット長の複数の乱数部分データを生成し、各分割データを構成する各分割部分データを元部分データと乱数部分データの排他

的論理和によって処理単位ビット長毎に生成して、所望の分割数の分割データを生成するとともに、

新たに発生させた乱数から処理単位ビット長の複数の乱数部分データを生成し、前記各分割部分データと該乱数部分データの排他的論理和により処理単位ビット長毎に再分割部分データを生成して、前記所望の分割数の再分割データを生成するデータ分割方法であり、

前記機密情報を前記秘密分散法を用いて複数の分割データに分割するデータ分割ステップと、

前記複数の分割データの一部を、前記利用者が保持するための分割データとして第 1 の記憶部に記憶させるとともに、前記複数の分割データの残りを、1 又は複数の第 2 の記憶部それぞれに記憶させるデータ記憶ステップと、

必要に応じて前記秘密分散法を用いて、前記第 2 の記憶部に記憶された各分割データのうち、復元可能な所定の個数の分割データの組み合わせから、複数の再分割データを作成するデータ再分割ステップと、

前記複数の再分割データの一部を新たな分割データとして前記第 1 の記憶部に記憶させるとともに、前記第 2 の記憶部に記憶された各分割データを無効にして、前記複数の再分割データの残りを新たな分割データとして前記第 2 の記憶部それぞれに記憶させるデータ再記憶ステップと、

を前記コンピュータに実行させることを特徴とする機密情報管理プログラム。

【請求項 1 2】

前記機密情報を使用する場合には、前記利用者が保持する分割データを取得し、該分割データと前記第 2 の記憶部に記憶された各分割データのうち前記所定の個数の分割データの組み合わせから前記秘密分散法を用いて前記機密情報を復元するデータ復元ステップを前記コンピュータに実行させることを特徴とする請求項 1 1 記載の機密情報管理プログラム。

【請求項 1 3】

前記機密情報を使用する場合には、前記第 2 の記憶部に記憶された各分割データのうち、前記所定の個数から前記利用者が保持する分割データの個数を引いた個数の分割データの組み合わせを前記利用者が有する端末に通信ネットワークを介して送信する分割データ送信ステップを前記コンピュータに実行させることを特徴とする請求項 1 1 記載の機密情報管理プログラム。

【請求項 1 4】

請求項 4 記載の機密情報管理システムから送信された分割データを用いて前記利用者の機密情報を使用するための端末が読み取り可能な機密情報管理システム用端末プログラムであって、

前記利用者が保持する分割データを取得し、該分割データと送信された分割データの組み合わせから前記秘密分散法を用いて前記機密情報を復元し、前記サービスを提供するシステムに通信ネットワークを介して送信するステップを

前記端末に実行させることを特徴とする機密情報管理システム用端末プログラム。

【書類名】 明細書

【発明の名称】 機密情報管理システム、機密情報管理方法、および機密情報管理プログラム、並びに機密情報管理システム用端末プログラム

【技術分野】**【0001】**

本発明は、利用者の機密情報を管理する機密情報管理システム、機密情報管理方法、および機密情報管理プログラム、並びに機密情報管理システム用端末プログラムに関する。

【背景技術】**【0002】**

IT (Information Technology) 技術の発展に伴って、パスワード、クレジット番号などが入った携帯電話および携帯情報端末、並びにPKI秘密鍵が入ったICカードなどを用いて、所望のサービスの提供を受ける機会が増えている。例えば、ユーザのパスワードを使用してログインし、情報を閲覧したり、ユーザのクレジットカード番号を使用して物品購入したりするようなサービスが普及している。

【0003】

このような機会において、ユーザが上述した機密情報（例えば、パスワード、クレジット番号およびPKI秘密鍵など）が記憶されている携帯電話、携帯情報端末およびICカードなどを紛失した場合には、紛失した旨を発行元に申告して、該機密情報を失効させ、新たに機密情報を再発行してもらう必要がある。

【非特許文献1】 電子認証システム推進検討会、“企業間電子商取引システムにおける電子認証システムの仕様に関するガイドライン”、[Online]、[平成16年1月20日検索]、インターネット<URL: <http://www.ecom.or.jp/home/g12.pdf>>

【発明の開示】**【発明が解決しようとする課題】****【0004】**

そのため、ユーザが保持する機密情報を紛失した際には、セキュリティ維持のため、紛失した機密情報を失効させるとともに、機密情報を変更しなければならないという課題がある。また、機密情報を変更するため、再発行まではサービスの提供を受けることができないという課題もある。

【0005】

本発明は、上記の課題を解決するためになされたものであり、ユーザが保持する携帯電話、携帯情報端末、ICカードを紛失しても、機密情報を変更することなくサービスの提供を受けることが可能な機密情報管理システム、機密情報管理方法、および機密情報管理プログラム、並びに機密情報管理システム用端末プログラムを提供することを目的とする。

【課題を解決するための手段】**【0006】**

上記目的を達成するため、請求項1記載の本発明は、利用者の機密情報を秘密分散法を用いて管理する機密情報管理システムであって、前記秘密分散法は、前記機密情報を所望の処理単位ビット長に基づいて所望の分割数の分割データに分割するデータ分割方法であり、前記機密情報を処理単位ビット長毎に区分けして、複数の元部分データを生成し、この複数の元部分データの各々に対応して、前記機密情報のビット長と同じまたはこれより短い長さの乱数から処理単位ビット長の複数の乱数部分データを生成し、各分割データを構成する各分割部分データを元部分データと乱数部分データの排他的論理和によって処理単位ビット長毎に生成して、所望の分割数の分割データを生成するとともに、新たに発生させた乱数から処理単位ビット長の複数の乱数部分データを生成し、前記各分割部分データと該乱数部分データの排他的論理和により処理単位ビット長毎に再分割部分データを生成して、前記所望の分割数の再分割データを生成するデータ分割方法であり、前記機密情報を前記秘密分散法を用いて複数の分割データに分割するデータ分割手段と、前記複数の分割データの一部を、前記利用者が保持するための分割データとして第1の記憶部に記憶

させるとともに、前記複数の分割データの残りを、1又は複数の第2の記憶部それぞれに記憶させるデータ記憶手段と、必要に応じて前記秘密分散法を用いて、前記第2の記憶部に記憶された各分割データのうち、復元可能な所定の個数の分割データの組み合わせから、複数の再分割データを作成するデータ再分割手段と、前記複数の再分割データの一部を新たな分割データとして前記第1の記憶部に記憶させるとともに、前記第2の記憶部に記憶された各分割データを無効にして、前記複数の再分割データの残りを新たな分割データとして前記第2の記憶部それぞれに記憶させるデータ再記憶手段と、を有することを特徴とする。

【0007】

請求項2記載の本発明は、請求項1記載の発明において、前記機密情報を使用する場合には、前記利用者が保持する分割データを取得し、該分割データと前記第2の記憶部に記憶された各分割データのうち前記所定の個数の分割データの組み合わせから前記秘密分散法を用いて前記機密情報を復元するデータ復元手段を有することを特徴とする。

【0008】

請求項3記載の本発明は、請求項2記載の発明において、前記機密情報を使用するときは、使用した事実を使用履歴情報として記憶する使用履歴記憶手段を有することを特徴とする。

【0009】

請求項4記載の本発明は、請求項1記載の発明において、前記機密情報を使用する場合には、前記第2の記憶部に記憶された各分割データのうち、前記所定の個数から前記利用者が保持する分割データの個数を引いた個数の分割データの組み合わせを前記利用者が有する端末に通信ネットワークを介して送信する分割データ送信手段を有することを特徴とする。

【0010】

請求項5記載の本発明は、請求項1乃至4のいずれか1項に記載の発明において、前記データ再分割手段は、前記所定の個数の分割データの組み合わせに含まれる各分割データを構成するそれぞれの分割部分データ同士の排他的論理和演算によって、前記利用者が保持した分割データを生成することを特徴とする。

【0011】

請求項6記載の本発明は、請求項1乃至5のいずれか1項に記載の発明において、前記秘密分散法は、前記各分割部分データと、該各分割部分データを生成する際に用いたそれぞれの乱数部分データに対応する新たな乱数部分データそれぞれとの排他的論理和演算により、各再分割部分データを生成することを特徴とする。

【0012】

請求項7記載の本発明は、前記秘密分散法は、さらに、前記各再分割部分データと、該各再分割部分データ生成前の各分割部分データを生成する際に用いた古い乱数部分データそれぞれとの排他的論理和演算により、前記再分割部分データから古い乱数部分データを消去することを特徴とする。

【0013】

請求項8記載の本発明は、請求項1乃至7のいずれか1項に記載の発明において、前記第1の記憶部に記憶される分割データを通信ネットワークを介して前記利用者が有する端末に送信する送信手段を有することを特徴とする。

【0014】

請求項9記載の本発明は、請求項1乃至8のいずれか1項に記載の発明において、前記機密情報を前記利用者が有する端末から通信ネットワークを介して受信する受信手段を有することを特徴とする機密情報管理システム。

【0015】

請求項10記載の本発明は、利用者の機密情報を秘密分散法を用いて管理する機密情報管理方法であって、前記秘密分散法は、前記機密情報を所望の処理単位ビット長に基づいて所望の分割数の分割データに分割するデータ分割方法であり、前記機密情報を処理単位

ビット長毎に区分けして、複数の元部分データを生成し、この複数の元部分データの各々に対応して、前記機密情報のビット長と同じまたはこれより短い長さの乱数から処理単位ビット長の複数の乱数部分データを生成し、各分割データを構成する各分割部分データを元部分データと乱数部分データの排他的論理和によって処理単位ビット長毎に生成して、所望の分割数の分割データを生成するとともに、新たに発生させた乱数から処理単位ビット長の複数の乱数部分データを生成し、前記各分割部分データと該乱数部分データの排他的論理和により処理単位ビット長毎に再分割部分データを生成して、前記所望の分割数の再分割データを生成するデータ分割方法であり、前記機密情報を前記秘密分散法を用いて複数の分割データに分割するデータ分割ステップと、前記複数の分割データの一部を、前記利用者が保持するための分割データとして第1の記憶部に記憶させるとともに、前記複数の分割データの残りを、1又は複数の第2の記憶部それぞれに記憶させるデータ記憶ステップと、必要に応じて前記秘密分散法を用いて、前記第2の記憶部に記憶された各分割データのうち、復元可能な所定の個数の分割データの組み合わせから、複数の再分割データを作成するデータ再分割ステップと、前記複数の再分割データの一部を新たな分割データとして前記第1の記憶部に記憶させるとともに、前記第2の記憶部に記憶された各分割データを無効にして、前記複数の再分割データの残りを新たな分割データとして前記第2の記憶部それぞれに記憶させるデータ再記憶ステップと、を有することを特徴とする。

【0016】

請求項11記載の本発明は、利用者の機密情報を秘密分散法を用いて管理するためのコンピュータが読み取り可能な機密情報管理プログラムであって、前記秘密分散法は、前記機密情報を所望の処理単位ビット長に基づいて所望の分割数の分割データに分割するデータ分割方法であり、前記機密情報を処理単位ビット長毎に区分けして、複数の元部分データを生成し、この複数の元部分データの各々に対応して、前記機密情報のビット長と同じまたはこれより短い長さの乱数から処理単位ビット長の複数の乱数部分データを生成し、各分割データを構成する各分割部分データを元部分データと乱数部分データの排他的論理和によって処理単位ビット長毎に生成して、所望の分割数の分割データを生成するとともに、新たに発生させた乱数から処理単位ビット長の複数の乱数部分データを生成し、前記各分割部分データと該乱数部分データの排他的論理和により処理単位ビット長毎に再分割部分データを生成して、前記所望の分割数の再分割データを生成するデータ分割方法であり、前記機密情報を前記秘密分散法を用いて複数の分割データに分割するデータ分割ステップと、前記複数の分割データの一部を、前記利用者が保持するための分割データとして第1の記憶部に記憶させるとともに、前記複数の分割データの残りを、1又は複数の第2の記憶部それぞれに記憶させるデータ記憶ステップと、必要に応じて前記秘密分散法を用いて、前記第2の記憶部に記憶された各分割データのうち、復元可能な所定の個数の分割データの組み合わせから、複数の再分割データを作成するデータ再分割ステップと、前記複数の再分割データの一部を新たな分割データとして前記第1の記憶部に記憶させるとともに、前記第2の記憶部に記憶された各分割データを無効にして、前記複数の再分割データの残りを新たな分割データとして前記第2の記憶部それぞれに記憶させるデータ再記憶ステップと、を前記コンピュータに実行させることを特徴とする。

【0017】

請求項12記載の本発明は、請求項11記載の発明において、前記機密情報を使用する場合には、前記利用者が保持する分割データを取得し、該分割データと前記第2の記憶部に記憶された各分割データのうち前記所定の個数の分割データの組み合わせから前記秘密分散法を用いて前記機密情報を復元するデータ復元ステップを前記コンピュータに実行させることを特徴とする。

【0018】

請求項13記載の本発明は、請求項11記載の発明において、前記機密情報を使用する場合には、前記第2の記憶部に記憶された各分割データのうち、前記所定の個数から前記利用者が保持する分割データの個数を引いた個数の分割データの組み合わせを前記利用者が有する端末に通信ネットワークを介して送信する分割データ送信ステップを前記コンピ

ユータに実行させることを特徴とする。

【0019】

請求項14記載の本発明は、請求項4記載の機密情報管理システムから送信された分割データを用いて前記利用者の機密情報を使用するための端末が読み取り可能な機密情報管理システム用端末プログラムであって、前記利用者が保持する分割データを取得し、該分割データと送信された分割データの組み合わせから前記秘密分散法を用いて前記機密情報を復元し、前記サービスを提供するシステムに通信ネットワークを介して送信するステップを前記端末に実行させることを特徴とする。

【発明の効果】

【0020】

本発明によれば、機密情報を秘密分散法を用いて複数に分割して、そのうちの一部をユーザに保持させるので、ユーザが保持する分割データの紛失があったとしても、残りの分割データから機密情報を復元できるとともに、秘密分散法を用いて新たに再分割データを生成し、該再分割データの一部を新たにユーザに保持させるので、機密情報の変更は不要である。

【0021】

この結果、ユーザが保持する分割データの紛失があったとしても、機密情報の再発行処理をすることなく、紛失の申告をするだけで、再びサービス提供を受けることができる。

【0022】

特に、本発明における秘密分散法は、機密情報を所望の処理単位ビット長に基づいて所望の分割数の分割データに分割するデータ分割方法であり、機密情報を処理単位ビット長毎に区分けして、複数の元部分データを生成し、この複数の元部分データの各々に対応して、機密情報のビット長と同じまたはこれより短い長さの乱数から処理単位ビット長の複数の乱数部分データを生成し、各分割データを構成する各分割部分データを元部分データと乱数部分データの排他的論理和によって処理単位ビット長毎に生成して、所望の分割数の分割データを生成するとともに、新たに発生させた乱数から処理単位ビット長の複数の乱数部分データを生成し、各分割部分データと該乱数部分データの排他的論理和により処理単位ビット長毎に再分割部分データを生成して、所望の分割数の再分割データを生成するので、機密情報を復元することなく、機密情報を再分割することができる。

【0023】

これにより、ユーザの機密情報をよりセキュアに管理することができる。

【発明を実施するための最良の形態】

【0024】

以下、本発明の実施の形態を図面を用いて説明する。

【0025】

<システム構成>

図1は、本発明の実施の形態に係る機密情報管理システム1が適用されるコンピュータシステム10全体の概略構成を示すブロック図である。

【0026】


図1に示すように、機密情報管理システム1は、インターネット等の通信ネットワーク4を介してユーザが備えるクライアント端末2（以下、単に端末とよぶ）と接続されるとともに、通信ネットワーク4を介してユーザに所定のサービスを提供するサービス提供システム5と接続されている。また、機密情報管理システム1は、ハードウェア的に互いに独立した複数（本実施の形態では2とする）のデータ保管用サーバコンピュータ（以下、単に保管サーバとよぶ）3a、3bと接続されている。

【0027】

尚、本実施の形態における機密情報とは、ユーザがサービス提供システム5を利用するために必要なパスワード、クレジットカード番号、PKI秘密鍵などの個人情報をいう。

【0028】

上記構成のコンピュータシステム10においては、端末2が所定のサービスをサービス



提供システム 5 から受ける際に必要とされる機密情報 S を機密情報管理システム 1 に送信すると、機密情報管理システム 1 において後述する独自の秘密分散アルゴリズムによる秘密分散法（以下、秘密分散法 A とよぶ）を用いて該機密情報 S を複数のデータに分割し、該分割データを保管サーバ 3 a, 3 b および端末 2 にそれぞれ送信し、保管させるようになっている。この結果、機密情報 S が機密情報管理システム 1 に登録されたことになり、ユーザはサービス利用の準備が整ったことになる。尚、図 1 では、機密情報管理システム 1 は、端末 2 からの機密情報 S を 3 つの分割データ D(1), D(2), D(3) に分割し、それぞれを複数の保管サーバ 3 a, 3 b および端末 2 に保管するようになっている。

【0029】

また、サービス利用時は、端末 2 から機密情報管理システム 1 に対して、分割データ D(3) を送信すると、機密情報管理システム 1 は、該分割データ D(3) および保管サーバ 3 a, 3 b の分割データ D(1), D(2) のうち任意の 2 つから秘密分散法 A を用いてもとの機密情報 S を復元し、該機密情報 S をサービス提供システム 5 に送信するようになっている。これにより、ユーザは、所定のサービスの提供を受けることができる。

【0030】

尚、本実施の形態においては、機密情報 S を 3 分割して保管する場合を例に説明するが、本発明は機密情報 S を 3 分割する場合に限定されるわけではなく、n 分割（n = 2 以上の整数）の場合にも適用されるものである。また、端末 2 に送信される分割データは 1 つとは限らず複数であってもよいものである。さらに、本実施の形態においては、分割データ D(1), D(2) を保管サーバ 3、分割データ D(3) を利用端末 2 に割り当てたが、どの分割データをどの保管サーバ 3 および利用端末 2 に割り当ててもよいものである。

【0031】

機密情報管理システム 1 は、詳しくは、機密情報 S から秘密分散法 A を用いて複数の分割データ D に分割する分割データ生成部 1 1、複数の分割データ D から秘密分散法 A を用いて元データ（機密情報）S を復元する元データ復元部 1 2、機密情報 S から複数の分割データ D を生成するために使用される乱数 R および再分割データ D' を生成するために使用される乱数 R' を発生させる乱数発生部 1 3、ユーザが保持する分割データを紛失した際には、秘密分散法 A を用いて保管サーバ 3 に保管された分割データから複数の再分割データ D' を生成する再分割データ生成部 1 4、機密情報管理システム 1 が機密情報 S を復元しサービス提供システム 5 に機密情報 S を送信した事実を使用履歴として生成する使用履歴生成部 1 5、並びに端末 2、保管サーバ 3 a, 3 b、およびサービス提供システム 5 とそれぞれとデータの送受信を行う通信部 1 6 を具備する構成となっている。

【0032】

また、端末 2 は、ユーザが携帯可能な携帯情報端末、携帯電話、IC カードなどの携帯記憶媒体などが想定されるが、他にモバイルを用途としないコンピュータ機器であってもよいものである。

【0033】

ここで、上述した機密情報管理システム 1、端末 2、保管サーバ 3 a, 3 b およびサービス提供システム 5 は、それぞれ少なくとも演算機能および制御機能を備えた中央演算装置（CPU）、プログラムやデータを格納する機能を有する RAM 等からなる主記憶装置（メモリ）を有する電子的な装置から構成されているものである。また、上記装置およびシステムは、主記憶装置の他、ハードディスクなどの補助記憶装置を具備していてもよい。

【0034】

また、本実施の形態に係る各種処理を実行するプログラムは、前述した主記憶装置またはハードディスクに格納されているものである。そして、このプログラムは、ハードディスク、フレキシブルディスク、CD-ROM、MO、DVD-ROM などのコンピュータ読み取り可能な記録媒体に記録することも、通信ネットワークを介して配信することも可能である。

【0035】

<秘密分散法 A>

ここで、本実施の形態における独自の秘密分散アルゴリズムによる秘密分散法 A について説明する。

【0036】

本実施形態における元データ（機密情報 S に相当する）の分割および復元では、元データを所望の処理単位ビット長に基づいて所望の分割数の分割データに分割するが、この場合の処理単位ビット長は任意の値に設定することができ、元データを処理単位ビット長毎に区分けして、この元部分データから分割部分データを分割数より 1 少ない数ずつ生成するので、元データのビット長が処理単位ビット長の（分割数-1）倍の整数倍に一致しない場合は、元データの末尾の部分に 0 を埋めるなどして元データのビット長を処理単位ビット長の（分割数-1）倍の整数倍に合わせることで本実施形態を適用することができる。

【0037】

また、上述した乱数も（分割数-1）個の元部分データの各々に対応して処理単位ビット長のビット長を有する（分割数-1）個の乱数部分データとして乱数発生部 13 から生成される。すなわち、乱数は処理単位ビット長毎に区分けされて、処理単位ビット長のビット長を有する（分割数-1）個の乱数部分データとして生成される。更に、元データは処理単位ビット長に基づいて所望の分割数の分割データに分割されるが、この分割データの各々も（分割数-1）個の元部分データの各々に対応して処理単位ビット長のビット長を有する（分割数-1）個の分割部分データとして生成される。すなわち、分割データの各々は、処理単位ビット長毎に区分けされて、処理単位ビット長のビット長を有する（分割数-1）個の分割部分データとして生成される。

【0038】

なお、以下の説明では、上述した元データ、乱数、分割データ、分割数および処理単位ビット長をそれぞれ S, R, D, n および b で表すとともに、また複数のデータや乱数などのうちの 1 つを表す変数として $i (=1 \sim n)$ および $j (=1 \sim n-1)$ を用い、（分割数 n-1）個の元部分データ、（分割数 n-1）個の乱数部分データ、および分割数 n 個の分割データ D のそれぞれのうちの 1 つをそれぞれ S(j), R(j) および D(i) で表記し、更に各分割データ D(i) を構成する複数の (n-1) の分割部分データを D(i, j) で表記するものとする。すなわち、S(j) は、元データ S の先頭から処理単位ビット長毎に区分けして 1 番から順に採番した時の j 番目の元部分データを表すものである。

【0039】

この表記を用いると、元データ、乱数データ、分割データとこれらをそれぞれ構成する元部分データ、乱数部分データ、分割部分データは、次のように表記される。

【0040】

元データ S = (n-1) 個の元部分データ S(j)
 $= S(1), S(2), \dots, S(n-1)$
 乱数 R = (n-1) 個の乱数部分データ R(j)
 $= R(1), R(2), \dots, R(n-1)$
 n 個の分割データ D(i) = D(1), D(2), ..., D(n)
 各分割部分データ D(i, j)
 $= D(1, 1), D(1, 2), \dots, D(1, n-1)$
 $D(2, 1), D(2, 2), \dots, D(2, n-1)$
 $\dots \quad \dots \quad \dots$
 $D(n, 1), D(n, 2), \dots, D(n, n-1)$
 $(i=1 \sim n), (j=1 \sim n-1)$

本実施形態は、上述したように処理単位ビット長毎に区分けされる複数の部分データに対して元部分データと乱数部分データの排他的論理和演算 (XOR) を行って、詳しくは、元部分データと乱数部分データの排他的論理和演算 (XOR) からなる定義式を用いて、元データの分割を行うことを特徴とするものであり、上述したデータ分割処理に多項式や剰

余演算を用いる方法に比較して、コンピュータ処理に適したビット演算である排他的論理和 (XOR) 演算を用いることにより高速かつ高性能な演算処理能力を必要とせず、大容量のデータに対しても簡単な演算処理を繰り返して分割データを生成することができるとともに、また分割データの保管に必要な記憶容量も分割数に比例した倍数の容量よりも小さくすることができる。更に、任意に定めた一定の長さ毎にデータの先頭から順に演算処理を行うストリーム処理により分割データが生成される。

【0041】

なお、本実施形態で使用する排他的論理和演算 (XOR) は、以下の説明では、「*」なる演算記号で表すことにするが、この排他的論理和演算のビット毎の演算規則での各演算結果は下記のとおりである。

【0042】

0 * 0 の演算結果は 0
 0 * 1 の演算結果は 1
 1 * 0 の演算結果は 1
 1 * 1 の演算結果は 0

また、XOR演算は交換法則、結合法則が成り立つ。すなわち、

$$a*b=b*a$$

$(a*b)*c=a*(b*c)$ が成り立つことが数学的に証明される。

【0043】

また、 $a*a=0$, $a*0=0*a=a$ が成り立つ。

【0044】

ここで a, b, c は同じ長さのビット列を表し、0 はこれらと同じ長さですべて「0」からなるビット列を表す。

【0045】

次に、フローチャートなどの図面も参照して、本実施の形態における秘密分散法 A の作用について説明するが、この説明の前に図 2 乃至 6、図 8 および図 10 のフローチャートに示す記号の定義について説明する。

【0046】

(1) $\prod_{i=1}^n A(i)$ は、 $A(1)*A(2)*\dots*A(n)$ を意味するものとする。

【0047】

(2) $c(j, i, k)$ を $(n-1) \times (n-1)$ 行列である $U[n-1, n-1] \times (P[n-1, n-1])^{(j-1)}$ の i 行 k 列の値と定義する。

【0048】

このとき $Q(j, i, k)$ を下記のように定義する。

【0049】

$c(j, i, k)=1$ のとき $Q(j, i, k)=R((n-1) \times m+k)$
 $c(j, i, k)=0$ のとき $Q(j, i, k)=0$

ただし、 m は $m \geq 0$ の整数を表す。

【0050】

(3) $U[n, n]$ とは、 $n \times n$ 行列であって、 i 行 j 列の値を $u(i, j)$ で表すと、

$i+j \leq n+1$ のとき $u(i, j)=1$
 $i+j > n+1$ のとき $u(i, j)=0$

である行列を意味するものとし、「上三角行列」ということとする。具体的には下記のような行列である。

【数 1】

$$U[3, 3] = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \quad U[4, 4] = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

【0051】

(4) $P[n, n]$ とは、 $n \times n$ 行列であって、 i 行 j 列の値を $p(i, j)$ で表すと、

$j=i+1$ のとき $p(i, j)=1$

$i=1, j=n$ のとき $p(i, j)=1$

上記以外るとき $p(i, j)=0$

である行列を意味するものとし、「回転行列」ということとする。具体的には下記のような行列であり、他の行列の右側からかけると当該他の行列の1列目を2列目へ、2列目を3列目へ、 \dots , $n-1$ 列目を n 列目へ、 n 列目を1列目へ移動させる作用がある。つまり、行列 P を他の行列に右側から複数回かけると、その回数分だけ各列を右方向へ回転させるように移動させることができる。

【数 2】

$$P[3, 3] = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \quad U[4, 4] = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

【0052】

(5) A, B を $n \times n$ 行列とすると、 $A \times B$ とは行列 A と B の積を意味するものとする。行列の成分同士の計算規則は通常の数学で用いるものと同じである。

【0053】

(6) A を $n \times n$ 行列とし、 i を整数とすると、 A^i とは行列 A の i 個の積を意味するものとする。また、 A^0 とは単位行列 E を意味するものとする。

【0054】

(7) 単位行列 $E[n, n]$ とは、 $n \times n$ 行列であって、 i 行 j 列の値を $e(i, j)$ で表すと、

$i=j$ のとき $e(i, j)=1$

上記以外るとき $e(i, j)=0$

である行列を意味するものとする。具体的には下記のような行列である。 A を任意の $n \times n$ 行列とすると

$$A \times E = E \times A = A$$

となる性質がある。

【数 3】

$$E[3, 3] = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad E[4, 4] = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

【0055】

次に、図2に示すフローチャートおよび図3および図4に示す具体的データなどを参照して、まず元データSの分割処理について説明する。これは、機密情報管理システム1の分割データ生成部11の機能を説明するものである。

【0056】

まず、元データSを機密情報管理システム1に与える（図2のステップS201）。なお、本例では、元データSは、16ビットの「10110010 00110111」とする。

【0057】

次に、機密情報管理システム1は、分割数nとして3と指示する（ステップS203）。なお、この分割数n=3に従って機密情報管理システム1で生成される3個の分割データをD(1), D(2), D(3)とする。この分割データD(1), D(2), D(3)は、すべて元データのビット長と同じ16ビット長のデータである。

【0058】

それから、元データSを分割するために使用される処理単位ビット長bを8ビットと決定する（ステップS205）。この処理単位ビット長bは、利用者が端末2から機密情報管理システム1に対して指定してもよいし、または機密情報管理システム1において予め定められた値を用いてもよい。なお、処理単位ビット長bは、任意のビット数でよいが、ここでは元データSを割り切れることができる8ビットとしている。従って、上記16ビットの「10110010 00110111」の元データSは、8ビットの処理単位ビット長で分けられた場合の2個の元分割データS(1)およびS(2)は、それぞれ「10110010」および「00110111」となる。

【0059】

次のステップS207では、元データSのビット長が8×2の整数倍であるか否かを判定し、整数倍でない場合には、元データSの末尾を0で埋めて、8×2の整数倍に合わせる。なお、本例のように処理単位ビット長bが8ビットおよび分割数nが3に設定された場合における分割処理は、元データSのビット長として16ビットに限られるものでなく、処理単位ビット長b×(分割数n-1)=8×2の整数倍の元データSに対して有効なものである。

【0060】

次に、ステップS209では、変数m、すなわち上述した整数倍を意味する変数mを0に設定する。本例のように、元データSが処理単位ビット長b×(分割数n-1)=8×2=16ビットである場合には、変数mは0であるが、2倍の32ビットの場合には、変数mは1となり、3倍の48ビットの場合には、変数mは2となる。

【0061】

次に、元データSの8×2×m+1ビット目から8×2ビット分のデータが存在するか否かが判定される（ステップS211）。これは、このステップS211以降に示す分割処理を元データSの変数mで特定される処理単位ビット長b×(分割数n-1)=8×2=16ビットに対して行った後、元データSとして次の16ビットがあるか否かを判定しているものである。本例のように元データSが16ビットである場合には、16ビットの元データSに対してステップS211以降の分割処理を1回行うと、後述するステップS219で変数mが+1されるが、本例の元データSでは変数mがm+1の場合に相当する17ビット以降のデータは存在しないので、ステップS211からステップS221に進むことになるが、今の場合は、変

数 m は0であるので、元データ S の $8 \times 2 \times m + 1$ ビット目は、 $8 \times 2 \times 0 + 1 = 1$ となり、元データ S の16ビットの1ビット目から 8×2 ビット分にデータが存在するため、ステップS213に進む。

【0062】

ステップS213では、変数 j を1から2(=分割数 $n-1$)まで変えて、元データ S の $8 \times (2 \times m + j - 1) + 1$ ビット目から8ビット分(=処理単位ビット長)のデータを元部分データ $S(2 \times m + j)$ に設定し、これにより元データ S を処理単位ビット長で分けした2(分割数 $n-1$)個の元部分データ $S(1), S(2)$ を次のように生成する。

【0063】

元データ $S = S(1), S(2)$

第1の元部分データ $S(1) = \text{「10110010」}$

第2の元部分データ $S(2) = \text{「00110111」}$

次に、変数 j を1から2(=分割数 $n-1$)まで変えて、乱数部分データ $R(2 \times m + j)$ に乱数発生部13から発生する8ビットの長さの乱数を設定し、これにより乱数 R を処理単位ビット長で分けした2(分割数 $n-1$)個の乱数部分データ $R(1), R(2)$ を次のように生成する(ステップS215)。

【0064】

乱数 $R = R(1), R(2)$

第1の乱数部分データ $R(1) = \text{「10110001」}$

第2の乱数部分データ $R(2) = \text{「00110101」}$

次に、ステップS217において、変数 i を1から3(=分割数 n)まで変えるとともに、更に各変数 i において変数 j を1から2(=分割数 $n-1$)まで変えながら、ステップS217に示す分割データを生成するための元部分データと乱数部分データの排他的論理和からなる定義式により複数の分割データ $D(i)$ の各々を構成する各分割部分データ $D(i, 2 \times m + j)$ を生成する。この結果、次に示すような分割データ D が生成される。

【0065】

分割データ D

= 3個の分割データ $D(i) = D(1), D(2), D(3)$

第1の分割データ $D(1)$

= 2個の分割部分データ $D(1, j) = D(1, 1), D(1, 2)$

= 「00110110」, 「10110011」

第2の分割データ $D(2)$

= 2個の分割部分データ $D(2, j) = D(2, 1), D(2, 2)$

= 「00000011」, 「00000010」

第3の分割データ $D(3)$

= 2個の分割部分データ $D(3, j) = D(3, 1), D(3, 2)$

= 「10110001」, 「00110101」

なお、各分割部分データ (i, j) を生成するためのステップS217に示す定義式は、本例のように分割数 $n=3$ の場合には、具体的には図4に示す表に記載されているものとなる。図4に示す表から、分割部分データ $D(1, 1)$ を生成するための定義式は $S(1) * R(1) * R(2)$ であり、 $D(1, 2)$ の定義式は $S(2) * R(1) * R(2)$ であり、 $D(2, 1)$ の定義式は $S(1) * R(1)$ であり、 $D(2, 2)$ の定義式は $S(2) * R(2)$ であり、 $D(3, 1)$ の定義式は $R(1)$ であり、 $D(3, 2)$ の定義式は $R(2)$ である。また、図4に示す表には $m > 0$ の場合の任意の整数についての一般的な定義式も記載されている。

【0066】

このように整数倍を意味する変数 $m=0$ の場合について分割データ D を生成した後、次に変数 m を1増やし(ステップS219)、ステップS211に戻り、変数 $m+1$ に該当する元データ S の17ビット以降について同様の分割処理を行おうとするが、本例の元データ S は16ビットであり、17ビット以降のデータは存在しないので、ステップS211からステップS221に進み、上述したように生成した分割データ $D(1), D(2), D(3)$ を保管サーバ3

及び端末 2 にそれぞれ保存して、分割処理を終了する。なお、このように保管された分割データ $D(1), D(2), D(3)$ はそれぞれ単独では元データが推測できない。

【0067】

ここで、上述した図 2 のフローチャートのステップ S 2 1 7 における定義式による分割データの生成処理、具体的には分割数 $n=3$ の場合の分割データの生成処理について詳しく説明する。

【0068】

まず、整数倍を意味する変数 $m=0$ の場合には、ステップ S 2 1 7 に示す定義式から各分割データ $D(i)=D(1) \sim D(3)$ の各々を構成する各分割部分データ $D(i, 2 \times m + j) = D(i, j)$ ($i=1 \sim 3, j=1 \sim 2$) は、次のようになる。

【0069】

$$D(1, 1) = S(1) * Q(1, 1, 1) * Q(1, 1, 2)$$

$$D(1, 2) = S(2) * Q(2, 1, 1) * Q(2, 1, 2)$$

$$D(2, 1) = S(1) * Q(1, 2, 1) * Q(1, 2, 2)$$

$$D(2, 2) = S(2) * Q(2, 2, 1) * Q(2, 2, 2)$$

$$D(3, 1) = R(1)$$

$$D(3, 2) = R(2)$$

上記の 6 つの式のうち上から 4 つの式に含まれる $Q(j, i, k)$ を具体的に求める。

【0070】

これは $c(j, i, k)$ を 2×2 行列である $U[2, 2] \times (P[2, 2])^{(j-1)}$ の i 行 k 列の値としたとき下記のように定義される。

【0071】

$$c(j, i, k) = 1 \text{ のとき } Q(j, i, k) = R(k)$$

$$c(j, i, k) = 0 \text{ のとき } Q(j, i, k) = 0$$

ここで、

$j=1$ のときは

【数 4】

$$U[2, 2] \times (P[2, 2])^{(j-1)} = U[2, 2] \times (P[2, 2])^0$$

$$= U[2, 2] \times E[2, 2]$$

$$= U[2, 2]$$

$$= \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

【0072】

$j=2$ のときは

【数 5】

$$\begin{aligned}
 U[2, 2] \times (P[2, 2])^{-(j-1)} &= U[2, 2] \times (P[2, 2])^{-1} \\
 &= U[2, 2] \times P[2, 2] \\
 &= \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \times \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\
 &= \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}
 \end{aligned}$$

【0073】

これを用いると、各分割部分データ $D(i, j)$ は次のような定義式により生成される。

【0074】

$$\begin{aligned}
 D(1, 1) &= S(1) * Q(1, 1, 1) * Q(1, 1, 2) = S(1) * R(1) * R(2) \\
 D(1, 2) &= S(2) * Q(2, 1, 1) * Q(2, 1, 2) = S(2) * R(1) * R(2) \\
 D(2, 1) &= S(1) * Q(1, 2, 1) * Q(1, 2, 2) = S(1) * R(1) * 0 = S(1) * R(1) \\
 D(2, 2) &= S(2) * Q(2, 2, 1) * Q(2, 2, 2) = S(2) * 0 * R(2) = S(2) * R(2)
 \end{aligned}$$

上述した各分割部分データ $D(i, j)$ を生成するための定義式は、図3にも図示されている。

。

【0075】

図3は、上述したように16ビットの元データ S を8ビットの処理単位ビット長に基づいて分割数 $n=3$ で3分割する場合の各データと定義式および各分割部分データから元データを復元する場合の計算式などを示す表である。

【0076】

ここで、上述した定義式により分割データ $D(1), D(2), D(3)$ および各分割部分データ $D(1, 1), D(1, 2), D(2, 1), D(2, 2), D(3, 1), D(3, 2)$ を生成する過程と定義式の一般形について説明する。

【0077】

まず、第1の分割データ $D(1)$ に対しては、第1の分割部分データ $D(1, 1)$ は、上述した定義式 $S(1) * R(1) * R(2)$ で定義され、第2の分割部分データ $D(1, 2)$ は定義式 $S(2) * R(1) * R(2)$ で定義される。なお、この定義式の一般形は、 $D(1, j)$ に対しては $S(j) * R(j) * R(j+1)$ であり、 $D(1, j+1)$ に対して $S(j+1) * R(j) * R(j+1)$ である（ j は奇数とする）。定義式に従って計算すると、 $D(1, 1)$ は00110110、 $D(1, 2)$ は10110011となるので、 $D(1)$ は00110110 10110011である。なお、定義式の一般形は、図4にまとめて示されている。

【0078】

また、第2の分割データ $D(2)$ に対しては、 $D(2, 1)$ は $S(1) * R(1)$ で定義され、 $D(2, 2)$ は $S(2) * R(2)$ で定義される。この定義式の一般形は、 $D(2, j)$ に対しては $S(j) * R(j)$ であり、 $D(2, j+1)$ に対しては $S(j+1) * R(j+1)$ である（ j は奇数とする）。定義式に従って計算すると、 $D(2, 1)$ は00000011、 $D(2, 2)$ は00000010となるので、 $D(2)$ は00000011 00000010である。

【0079】

更に第3の分割データ $D(3)$ に対しては、 $D(3, 1)$ は $R(1)$ で定義され、 $D(3, 2)$ は $R(2)$ で定義される。この定義式の一般形は、 $D(3, j)$ に対しては $R(j)$ であり、 $D(3, j+1)$ に対しては $R(j+1)$ である（ j は奇数とする）。定義式に従って計算すると、 $D(3, 1)$ は10110001、 $D(3, 2)$ は0110101となるので、 $D(3)$ は10110001 0110101である。

【0080】

上記説明は、 $S, R, D(1), D(2), D(3)$ の長さを16ビットとしたが、データの先頭から上記分割処理を繰り返すことにより、どのような長さの元データ S からでも分割データ $D(1), D($

2), D(3)を生成することができる。また、処理単位ビット長bは任意にとることができ、元データSの先頭から順にb×2の長さ毎に上記分割処理を繰り返すことにより任意の長さの元データ、具体的には処理単位ビット長b×2の整数倍の長さの元データに対して適用することができる。なお、元データSの長さが処理単位ビット長b×2の整数倍でない場合は、例えば、データ末尾の部分を0で埋めるなどして元データSの長さを処理単位ビット長b×2の整数倍に合わせるにより上述した本実施形態の分割処理を適用することができる。

【0081】

次に、図3の右側に示す表を参照して、分割データから元データを復元する処理について説明する。これは、機密情報管理システム1の元データ復元部13の機能を説明するものである。

【0082】

まず、機密情報管理システム1に元データSの復元を要求する。機密情報管理システム1は、保管サーバ3および端末2から分割データD(1), D(2), D(3)を取得し、この取得した分割データD(1), D(2), D(3)から次に示すように元データSを復元する。

【0083】

まず、分割部分データD(2, 1), D(3, 1)から第1の元部分データS(1)を次のように生成することができる。

【0084】

$$\begin{aligned} D(2, 1) * D(3, 1) &= (S(1) * R(1)) * R(1) \\ &= S(1) * (R(1) * R(1)) \\ &= S(1) * 0 \\ &= S(1) \end{aligned}$$

具体的に計算すると、D(2, 1)は00000011, D(3, 1)は10110001なので、S(1)は10110010となる。

【0085】

また、別の分割部分データから次のように第2の元部分データS(2)を生成することができる。

【0086】

$$\begin{aligned} D(2, 2) * D(3, 2) &= (S(2) * R(2)) * R(2) \\ &= S(2) * (R(2) * R(2)) \\ &= S(2) * 0 \\ &= S(2) \end{aligned}$$

具体的に計算すると、D(2, 2)は00000010, D(3, 2)は00110101なので、S(2)は00110111となる。

【0087】

一般に、jを奇数として、

$$\begin{aligned} D(2, j) * D(3, j) &= (S(j) * R(j)) * R(j) \\ &= S(j) * (R(j) * R(j)) \\ &= S(j) * 0 \\ &= S(j) \end{aligned}$$

であるから、D(2, j)*D(3, j)を計算すれば、S(j)が求まる。

【0088】

また、一般に、jを奇数として、

$$\begin{aligned} D(2, j+1) * D(3, j+1) &= (S(j+1) * R(j+1)) * R(j+1) \\ &= S(j+1) * (R(j+1) * R(j+1)) \\ &= S(j+1) * 0 \\ &= S(j+1) \end{aligned}$$

であるから、D(2, j+1)*D(3, j+1)を計算すれば、S(j+1)が求まる。

【0089】

次に、D(1), D(3)を取得してSを復元する場合には、次のようになる。

【0090】

$$\begin{aligned} D(1,1)*D(3,1)*D(3,2) &= (S(1)*R(1)*R(2))*R(1)*R(2) = S(1)*(R(1)*R(1))*(R(2)*R(2)) \\ &= S(1)*0*0 \\ &= S(1) \end{aligned}$$

であるから、D(1,1)*D(3,1)*D(3,2)を計算すれば、S(1)が求まる。具体的に計算すると、D(1,1)は00110110, D(3,1)は10110001, D(3,2)は00110101なので、S(1)は10110010となる。

【0091】

また同様に、

$$\begin{aligned} D(1,2)*D(3,1)*D(3,2) &= (S(2)*R(1)*R(2))*R(1)*R(2) \\ &= S(2)*(R(1)*R(1))*(R(2)*R(2)) \\ &= S(2)*0*0 \\ &= S(2) \end{aligned}$$

であるから、D(1,2)*D(3,1)*D(3,2)を計算すれば、S(2)が求まる。具体的に計算すると、D(1,2)は10110011, D(3,1)は10110001, D(3,2)は00110101なので、S(2)は00110111となる。

【0092】

一般に、jを奇数として、

$$\begin{aligned} D(1,j)*D(3,j)*D(3,j+1) &= (S(j)*R(j)*R(j+1))*R(j)*R(j+1) \\ &= S(j)*(R(j)*R(j))*(R(j+1)*R(j+1)) \\ &= S(j)*0*0 \\ &= S(j) \end{aligned}$$

であるから、D(1,j)*D(3,j)*D(3,j+1)を計算すれば、S(j)が求まる。

【0093】

また、一般に、jを奇数として、

$$\begin{aligned} D(1,j+1)*D(3,j)*D(3,j+1) &= (S(j+1)*R(j)*R(j+1))*R(j)*R(j+1) \\ &= S(j+1)*(R(j)*R(j))*(R(j+1)*R(j+1)) \\ &= S(j+1)*0*0 \\ &= S(j+1) \end{aligned}$$

であるから、D(1,j+1)*D(3,j)*D(3,j+1)を計算すれば、S(j+1)が求まる。

【0094】

次に、D(1), D(2)を取得してSを復元する場合には、次のようになる。

【0095】

$$\begin{aligned} D(1,1)*D(2,1) &= (S(1)*R(1)*R(2))*(S(1)*R(1)) \\ &= (S(1)*S(1))*(R(1)*R(1))*R(2) \\ &= 0*0*R(2) \\ &= R(2) \end{aligned}$$

であるから、D(1,1)*D(2,1)を計算すれば、R(2)が求まる。具体的に計算すると、D(1,1)は00110110, D(2,1)は00000011なので、R(2)は00110101となる。

【0096】

また同様に、

$$\begin{aligned} D(1,2)*D(2,2) &= (S(2)*R(1)*R(2))*(S(2)*R(2)) \\ &= (S(2)*S(2))*R(1)*(R(2)*R(2)) \\ &= 0*R(1)*0 \\ &= R(1) \end{aligned}$$

であるから、D(1,2)*D(2,2)を計算すれば、R(1)が求まる。具体的に計算すると、D(1,2)は10110011, D(2,2)は00000010なので、R(1)は10110001となる。

【0097】

このR(1), R(2)を使用してS(1), S(2)を求める。

【 0 0 9 8 】

$$\begin{aligned}
 D(2,1)*R(1) &= (S(1)*R(1))*R(1) \\
 &= S(1)*(R(1)*R(1)) \\
 &= S(1)*0 \\
 &= S(1)
 \end{aligned}$$

であるから、 $D(2,1)*R(1)$ を計算すれば、 $S(1)$ が求まる。具体的に計算すると、 $D(2,1)$ は0000011, $R(1)$ は10110001なので、 $S(1)$ は10110010となる。

【 0 0 9 9 】

また同様に、

$$\begin{aligned}
 D(2,2)*R(2) &= (S(2)*R(2))*R(2) \\
 &= S(2)*(R(2)*R(2)) \\
 &= S(2)*0 \\
 &= S(2)
 \end{aligned}$$

であるから $D(2,2)*R(2)$ を計算すれば $S(2)$ が求まる。具体的に計算すると $D(2,2)$ は00000010, $R(2)$ は00110101なので、 $S(2)$ は00110111となる。

【 0 1 0 0 】

一般に、 j を奇数として、

$$\begin{aligned}
 D(1,j)*D(2,j) &= (S(j)*R(j)*R(j+1))*(S(j)*R(j)) \\
 &= (S(j)*S(j))*(R(j)*R(j))*R(j+1) \\
 &= 0*0*R(j+1) \\
 &= R(j+1)
 \end{aligned}$$

であるから $D(1,j)*D(2,j)$ を計算すれば $R(j+1)$ が求まる。

【 0 1 0 1 】

また同様に、

$$\begin{aligned}
 D(1,j+1)*D(2,j+1) &= (S(j+1)*R(j)*R(j+1))*(S(j+1)*R(j+1)) \\
 &= (S(j+1)*S(j+1))*R(j)*(R(j+1)*R(j+1)) \\
 &= 0*R(j)*0 \\
 &= R(j)
 \end{aligned}$$

であるから $D(1,j+1)*D(2,j+1)$ を計算すれば $R(j)$ が求まる。

【 0 1 0 2 】

この $R(j), R(j+1)$ を使用して $S(j), S(j+1)$ を求める。

【 0 1 0 3 】

$$\begin{aligned}
 D(2,j)*R(j) &= (S(j)*R(j))*R(j) \\
 &= S(j)*(R(j)*R(j)) \\
 &= S(j)*0 \\
 &= S(j)
 \end{aligned}$$

であるから $D(2,j)*R(j)$ を計算すれば $S(j)$ が求まる。

【 0 1 0 4 】

また同様に、

$$\begin{aligned}
 D(2,j+1)*R(j+1) &= (S(j+1)*R(j+1))*R(j+1) \\
 &= S(j+1)*(R(j+1)*R(j+1)) \\
 &= S(j+1)*0 \\
 &= S(j+1)
 \end{aligned}$$

であるから $D(2,j+1)*R(j+1)$ を計算すれば $S(j+1)$ が求まる。

【 0 1 0 5 】

上述したように、元データの先頭から処理単位ビット長 b に基づいて分割処理を繰り返して行って、分割データを生成した場合には、3つの分割データ $D(1), D(2), D(3)$ のすべてを用いなくても、3つの分割データのうち、2つの分割データを用いて上述したように元データを復元することができる。

【 0 1 0 6 】

本発明の他の方法として、乱数Rのビット長を元データSのビット長よりも短いものを使用して、元データの分割処理を行うことができる。

【0107】

すなわち、上述した乱数RはS, D(1), D(2), D(3)と同じビット長のデータとしたが、乱数Rを元データSのビット長より短いものとし、分割データD(1), D(2), D(3)の生成にこの短いビット長の乱数Rを繰り返し用いるものである。

【0108】

尚、本実施の形態に係る機密情報管理システム1においては、3つの分割データD(1), D(2), D(3)を生成するようになっていたので、分割数が3の場合について説明したが、秘密分散法Aは、分割数がnの場合にも適用できるものである。

【0109】

次に、図5に示すフローチャートを参照して、分割数がnで、処理単位ビット長がbである場合の一般的な分割処理について説明する。

【0110】

まず、元データSを機密情報管理システム1に与える(ステップS401)。また、機密情報管理システム1に、分割数n($n \geq 3$ である任意の整数)を指示する(ステップS403)。処理単位ビット長bを決定する(ステップS405)。なお、bは0より大きい任意の整数である。次に、元データSのビット長が $b \times (n-1)$ の整数倍であるか否かを判定し、整数倍でない場合には、元データSの末尾を0で埋める(ステップS407)。また、整数倍を意味する変数mを0に設定する(ステップS409)。

【0111】

次に、元データSの $b \times (n-1) \times m+1$ ビット目から $b \times (n-1)$ ビット分のデータが存在するかが判定される(ステップS411)。この判定の結果、データが存在しない場合は、ステップS421に進むことになるが、今の場合は、ステップS409で変数mは0に設定された場合であるので、データが存在するため、ステップS413に進む。

【0112】

ステップS413では、変数jを1からn-1まで変えて、元データSの $b \times ((n-1) \times m+j-1)+1$ ビット目からbビット分のデータを元部分データS(($(n-1) \times m+j$))に設定する処理を繰り返す、これにより元データSを処理単位ビット長bで分けした(n-1)個の元部分データS(1), S(2), ..., S(n-1)が生成される。

【0113】

次に、変数jを1からn-1まで変えて、乱数部分データR(($(n-1) \times m+j$))に乱数発生部15から発生する処理単位ビット長bの乱数を設定し、これにより乱数Rを処理単位ビット長bで分けしたn-1個の乱数部分データR(1), R(2), ..., R(n-1)が生成される(ステップS415)。

【0114】

次に、ステップS417において、変数iを1からnまで変えるとともに、更に各変数iにおいて変数jを1からn-1まで変えながら、ステップS417に示す分割データを生成するための定義式により複数の分割データD(i)の各々を構成する各分割部分データD(i, ($(n-1) \times m+j$))を生成する。この結果、次に示すような分割データDが生成される。

【0115】

分割データD

=n個の分割データD(i)=D(1), D(2), ..., D(n)

第1の分割データD(1)

=n-1個の分割部分データD(1, j)=D(1, 1), D(1, 2), ..., D(1, n-1)

第2の分割データD(2)

=n-1個の分割部分データD(2, j)=D(2, 1), D(2, 2), ..., D(2, n-1)

...

...

...

...

...

...

第nの分割データD(n)

=n-1個の分割部分データ $D(n, j)=D(n, 1), D(n, 2), \dots, D(n, n-1)$

このように変数 $m=0$ の場合について分割データ D を生成した後、次に変数 m を1増やし（ステップS419）、ステップS411に戻り、変数 $m=1$ に該当する元データ S の $b \times (n-1)$ ビット以降について同様の分割処理を行う。最後にステップS411の判定の結果、元データ S にデータがなくなった場合、ステップS411からステップS421に進み、上述したように生成した分割データ $D(1), \dots, D(n)$ を保管サーバ3および端末2にそれぞれ保存して、分割処理を終了する。

【0116】

さて、上述した実施形態においては、この分割データのみから、それを構成する部分データ間の演算を行うことによって乱数成分が失われる場合がある。即ち、例えば3分割の場合、各分割部分データは次のように定義される。

【0117】

$$D(1, 1)=S(1)*R(1)*R(2), \quad D(1, 2)=S(2)*R(1)*R(2), \quad \dots$$

$$D(2, 1)=S(1)*R(1), \quad D(2, 2)=S(2)*R(2), \quad \dots$$

$$D(3, 1)=R(1), \quad D(3, 2)=R(2), \quad \dots$$

$D(1)$ について見ると、例えば、 $D(1, 1)$ 、 $D(1, 2)$ が取得できると、

$$\begin{aligned} D(1, 1)*D(1, 2) &= (S(1)*R(1)*R(2)) * (S(2)*R(1)*R(2)) \\ &= S(1)*S(2)*((R(1)*R(1))*(R(2)*R(2))) \\ &= S(1)*S(2)*0*0 \\ &= S(1)*S(2) \end{aligned}$$

となる。一般には $D(1, j)*D(1, j+1)=S(j)*S(j+1)$ である。ここで j は $j=2 \times m+1$ 、 m は $m \geq 0$ の任意の整数である。

【0118】

$D(1, 1)$ 、 $D(1, 2)$ は、上記の定義より、元データと乱数の演算により生成されたものであり、 $D(1, 1)$ 、 $D(1, 2)$ それぞれを見ても元データの内容は分からないが、 $D(1, 1)*D(1, 2)$ の演算を行うことにより $S(1)*S(2)$ が算出される。これは元データそのものではないが、乱数成分を含んでいない。

【0119】

このように乱数成分が失われると、個々の元部分データについて、例えば $S(2)$ の一部が既知である場合には $S(1)$ の一部が復元可能となるので、安全ではないと考えられる。例えば、元データが標準化されたデータフォーマットに従ったデータであって、 $S(2)$ がそのデータフォーマット中のヘッダ情報やパディング（例えば、データ領域の一部を0で埋めたもの）などを含む部分であった場合には、これらのデータフォーマット固有のキーワードや固定文字列などを含むため、その内容は予測され得る。また、 $S(2)$ のうち既知の部分と $S(1)*S(2)$ の値から、 $S(1)$ の一部が復元可能である。

【0120】

この問題を解決する方法は以下の通りである。図6における $D(1, j+1)$ と $D(2, j+1)$ は、図4における $D(1, j+1)$ と $D(2, j+1)$ を入れ替えたものである。ここで j は $j=2 \times m+1$ 、 m は $m \geq 0$ の任意の整数である。

【0121】

この場合、個々の分割データのみでは、それを構成する分割部分データ間で演算を行っても乱数成分が失われない。これは、図6より

$$\begin{aligned} D(1, j)*D(1, j+1) &= (S(j)*R(j)*R(j+1)) * (S(j+1)*R(j+1)) \\ &= S(j)*S(j+1)*R(j)*((R(j+1)*R(j+1))) \\ &= S(j)*S(j+1)*R(j)*0 \\ &= S(j)*S(j+1)*R(j) \end{aligned}$$

$$\begin{aligned} D(2, j)*D(2, j+1) &= (S(j)*R(j)) * (S(j+1)*R(j)*R(j+1)) \\ &= S(j)*S(j+1)*((R(j)*R(j)))*R(j+1) \\ &= S(j)*S(j+1)*0*R(j+1) \\ &= S(j)*S(j+1)*R(j+1) \end{aligned}$$

$D(3, j) * D(3, j+1) = R(j) * R(j+1)$
となるからである。

【0 1 2 2】

また、この場合、3つの分割データのうち2つから、元データを復元することができるという特性は失われていない。これは、 $D(1)$ 、 $D(2)$ を取得して S を復元する場合には、図6における $D(1)$ 、 $D(2)$ は、図4における $D(1)$ 、 $D(2)$ を構成する分割部分データを入れ替えたものにすぎないので、明らかにこれらから元データを復元することができ、また、 $D(1)$ と $D(3)$ または $D(2)$ と $D(3)$ を取得して S を復元する場合には、 $D(3)$ は乱数のみからなる分割データであるので、 $D(1)$ または $D(2)$ の分割部分データ毎に必要な個数の乱数との排他的論理和演算を行うことにより、乱数部分を消去して元データを復元することができるからである。

【0 1 2 3】

次に、一旦分割された分割データにさらに乱数を与えて新たな分割データ（再分割データ）を生成する再分割処理について説明する。これは、ユーザが保持する分割データを紛失した場合における機密情報管理システム1の再分割データ生成部14の機能を説明するものであるが、これに関しても、分割数が3の場合を例に説明する。尚、本実施の形態における再分割処理は、2つの方法があるので、以下、それぞれについて説明する。

【0 1 2 4】

（乱数追加注入方式）

図7は、乱数追加注入方式におけるデータ再分割処理の概要を説明するフローチャート図である。同図によれば、まず分割データ $D(1)$ 、 $D(2)$ 、 $D(3)$ を取得し（ステップS501）、次に、乱数発生部13で再分割の際に用いる乱数 R' を発生させる（ステップS503）。

【0 1 2 5】

次に、分割データ $D(1)$ 、 $D(2)$ 、 $D(3)$ それぞれに乱数 R' を所定のルールで注入する（ステップS505）。これは、後述するようなルールにより分割データ $D(1)$ 、 $D(2)$ 、 $D(3)$ の分割部分データと乱数 R' の乱数部分データの排他的論理和をとり、新たな分割データ $D'(1)$ 、 $D'(2)$ 、 $D'(3)$ を生成するものである（ステップS507）。

【0 1 2 6】

図8は、元データ S を、元データの半分の長さの処理単位ビット長 b に基づいて分割数 $n=3$ で3分割する場合の分割部分データの定義式、乱数の再注入後の分割部分データの定義式、および各分割部分データから元データを復元する場合の計算式などを示す表である。

【0 1 2 7】

ここで、分割部分データ $D(i, j)$ の定義式について説明する。

【0 1 2 8】

まず、第1の分割データ $D(1)$ に対しては、図6に示すように、第1の分割部分データ $D(1, 1)$ は、定義式 $S(1) * R(1) * R(2)$ で定義され、第2の分割部分データ $D(1, 2)$ は定義式 $S(2) * R(2)$ で定義される。なお、この定義式の一般形は、 $D(1, j)$ に対しては $S(j) * R(j) * R(j+1)$ であり、 $D(1, j+1)$ に対しては $S(j+1) * R(j+1)$ である（ j は奇数とする）。

【0 1 2 9】

また、第2の分割データ $D(2)$ に対しては、図6に示すように、 $D(2, 1)$ は $S(1) * R(1)$ で定義され、 $D(2, 2)$ は $S(2) * R(1) * R(2)$ で定義される。この定義式の一般形は、 $D(2, j)$ に対しては $S(j) * R(j)$ であり、 $D(2, j+1)$ に対しては $S(j+1) * R(j) * R(j+1)$ である（ j は奇数とする）。

【0 1 3 0】

更に第3の分割データ $D(3)$ に対しては、図6に示すように、 $D(3, 1)$ は $R(1)$ で定義され、 $D(3, 2)$ は $R(2)$ で定義される。この定義式の一般形は、 $D(3, j)$ に対しては $R(j)$ であり、 $D(3, j+1)$ に対しては $R(j+1)$ である（ j は奇数とする）。

【0 1 3 1】

次に、新たな乱数 R' 注入後の分割部分データ $D'(i, j)$ の定義式について説明する。

【0 1 3 2】

まず、第1の分割データD'(1)に対しては、図8に示すように、第1の分割部分データD'(1,1)は、定義式 $D(1,1)*R'(1)*R'(2)$ 、即ち、 $S(1)*R(1)*R(2)*R'(1)*R'(2)$ で定義され、第2の分割部分データD'(1,2)は、定義式 $D(1,2)*R'(2)$ 、即ち、 $S(2)*R(2)*R'(2)$ で定義される。なお、この定義式の一般形は、D'(1,j)に対しては $D(1,j)*R'(j)*R'(j+1)$ であり、D'(1,j+1)に対して $D(1,j+1)*R'(j+1)$ である(jは奇数とする)。

【0133】

また、第2の分割データD'(2)に対しては、図8に示すように、D'(2,1)は $D(2,1)*R'(1)$ 、即ち、 $S(1)*R(1)*R'(1)$ で定義され、D'(2,2)は $D(2,2)*R'(1)*R'(2)$ 、即ち、 $S(2)*R(1)*R(2)*R'(1)*R'(2)$ で定義される。この定義式の一般形は、D'(2,j)に対しては $D(2,j)*R'(j)$ であり、D'(2,j+1)に対しては $D(2,j+1)*R'(j)*R'(j+1)$ である(jは奇数とする)。

【0134】

また、第3の分割データD'(3)に対しては、図8に示すように、D'(3,1)は $D(3,1)*R'(1)$ 、即ち、 $R(1)*R'(1)$ で定義され、D'(3,2)は $D(3,2)*R'(2)$ 、即ち、 $R(2)*R'(2)$ で定義される。この定義式の一般形は、D'(3,j)に対しては $D(3,j)*R'(j)*R'(j+1)$ であり、D'(3,j+1)に対しては $D(3,j+1)*R'(j+1)$ である(jは奇数とする)。

【0135】

このように、再分割部分データD'(i,j)はそれぞれ、分割部分データD(i,j)に、分割部分データD(i,j)の定義式で注入されていた乱数部分データR(j)に対応する乱数部分データR'(j)を注入して排他的論理和を計算して求めるものである。

【0136】

尚、ユーザが保持する分割データを紛失した場合には、上述した分割データD(1),D(2),D(3)のうちいずれか1つを紛失しているので、紛失した分割データに関しては、残りの2つの分割データから復元し、その後、再分割データを生成する必要がある。ここで、残りの2つの分割データから紛失した分割データを生成する方法について説明する。

【0137】

まず、分割データD(3)を紛失し、分割データD(1),D(2)から分割データD(3)を生成する場合について説明する。具体的には、図8の例で説明すると

$$\begin{aligned} D(1,1)*D(2,1) &= ((S(1)*R(1)*R(2))*(S(1)*R(1))) \\ &= R(2)*(S(1)*S(1))*(R(1)*R(1)) \\ &= R(2) \end{aligned}$$

$$\begin{aligned} D(1,2)*D(2,2) &= ((S(2)*R(2))*(S(2)*R(1)*R(2))) \\ &= R(1)*(S(2)*S(2))*(R(2)*R(2)) \\ &= R(1) \end{aligned}$$

であり、また、 $D(3,1)=R(1)$ 、 $D(3,2)=R(2)$ であるから、 $D(1,1)*D(2,1)$ および $D(1,2)*D(2,2)$ から分割データD(3)を生成することができる。

【0138】

また、分割データD(1)を紛失し、分割データD(2),D(3)から分割データD(1)を生成する場合については、

$$D(1,1)=D(2,1)*R(2)$$

$$D(1,2)=D(2,2)*R(1)$$

であり、また、 $D(3,1)=R(1)$ 、 $D(3,2)=R(2)$ であるから、 $D(2,1)*R(2)$ および $D(2,2)*R(1)$ から分割データD(1)を生成することができる。

【0139】

また、分割データD(2)を紛失し、分割データD(1),D(3)から分割データD(2)を生成する場合については、

$$D(2,1)=D(1,1)*R(2)$$

$$D(2,2)=D(1,2)*R(1)$$

であり、また、 $D(3,1)=R(1)$ 、 $D(3,2)=R(2)$ であるから、分割データD(1),D(3)から分割データD(2)を生成することができる。

【0140】

次に、図8の右側に示す表を参照して、再分割データから元データを復元する処理について説明する。これは、ユーザが再分割データを受け取った後のサービス利用時において、機密情報管理システム1の元データ復元部12の機能を説明するものである。

【0141】

まず、分割部分データ $D'(2,1)$ 、 $D'(3,1)$ から第1の元部分データ $S(1)$ を次のように生成することができる。

【0142】

$$\begin{aligned} D'(2,1) * D'(3,1) &= (S(1) * R(1) * R'(1)) * (R(1) * R'(1)) \\ &= S(1) * (R(1) * R(1)) * (R'(1) * R'(1)) \\ &= S(1) * 0 * 0 \\ &= S(1) \end{aligned}$$

また、別の分割部分データから次のように第2の元部分データ $S(2)$ を生成することができる。

【0143】

$$\begin{aligned} D'(2,2) * D'(3,1) * D'(3,2) &= (S(2) * R(1) * R(2) * R'(1) * R'(2)) * \\ &\quad (R(1) * R'(1)) * (R(2) * R'(2)) \\ &= S(2) * (R(1) * R(1)) * (R(2) * R(2)) * \\ &\quad (R'(1) * R'(1)) * (R'(2) * R'(2)) \\ &= S(2) * 0 * 0 * 0 * 0 \\ &= S(2) \end{aligned}$$

一般に、 j を奇数として、

$$\begin{aligned} D'(2,j) * D'(3,j) &= (S(j) * R(j) * R'(j)) * (R(j) * R'(j)) \\ &= S(j) * (R(j) * R(j)) * (R'(j) * R'(j)) \\ &= S(j) * 0 * 0 \\ &= S(j) \end{aligned}$$

であるから、 $D'(2,j) * D'(3,j)$ を計算すれば、 $S(j)$ が求まる。

【0144】

また、一般に、 j を奇数として、

$$\begin{aligned} D'(2,j+1) * D'(3,j) * D'(3,j+1) &= (S(j+1) * R(j) * R(j+1) * R'(j) * R'(j+1)) * \\ &\quad (R(j) * R'(j)) * (R(j+1) * R'(j+1)) \\ &= S(j+1) * ((R(j) * R(j)) * (R(j+1) * R(j+1)) * \\ &\quad * (R'(j) * R'(j)) * (R'(j+1) * R'(j+1))) \\ &= S(j+1) * 0 * 0 * 0 * 0 \\ &= S(j+1) \end{aligned}$$

であるから、 $D'(2,j+1) * D'(3,j) * D'(3,j+1)$ を計算すれば、 $S(j+1)$ が求まる。

【0145】

次に、 $D'(1)$ 、 $D'(3)$ を取得して S を復元する場合には、次のようになる。

【0146】

$$\begin{aligned} D'(1,1) * D'(3,1) * D'(3,2) &= (S(1) * R(1) * R(2) * R'(1) * R'(2)) * \\ &\quad (R(1) * R'(1)) * (R(2) * R'(2)) \\ &= S(1) * (R(1) * R(1)) * (R(2) * R(2)) * \\ &\quad (R'(1) * R'(1)) * (R'(2) * R'(2)) \\ &= S(1) * 0 * 0 * 0 * 0 \\ &= S(1) \end{aligned}$$

であるから、 $D'(1,1) * D'(3,1) * D'(3,2)$ を計算すれば、 $S(1)$ が求まる。

【0147】

また同様に、

$$\begin{aligned} D'(1,2) * D'(3,2) &= (S(2) * R(2) * R'(2)) * (R(2) * R'(2)) \\ &= S(2) * (R(2) * R(2)) * (R'(2) * R'(2)) \end{aligned}$$

$$=S(2)*0*0$$

$$=S(2)$$

であるから、 $D'(1,2)*D'(3,2)$ を計算すれば、 $S(2)$ が求まる。

【0 1 4 8】

一般に、 j を奇数として、

$$D'(1,j)*D'(3,j)*D'(3,j+1)=(S(j)*R(j)*R(j+1)*R'(j)*R'(j+1))*$$

$$(R(j)*R'(j))*(R(j+1)*R'(j+1))$$

$$=S(j)*(R(j)*R(j))*(R(j+1)*R(j+1))*$$

$$(R'(j)*R'(j))*(R'(j+1)*R'(j+1))$$

$$=S(j)*0*0*0$$

$$=S(j)$$

であるから、 $D'(1,j)*D'(3,j)*D'(3,j+1)$ を計算すれば、 $S(j)$ が求まる。

【0 1 4 9】

また、一般に、 j を奇数として、

$$D'(1,j+1)*D'(3,j+1)=(S(j+1)*R(j+1)*R'(j+1))*(R(j+1)*R'(j+1))$$

$$=S(j+1)*(R(j+1)*R(j+1))*(R'(j+1)*R'(j+1))$$

$$=S(j+1)*0*0$$

$$=S(j+1)$$

であるから、 $D'(1,j+1)*D'(3,j+1)$ を計算すれば、 $S(j+1)$ が求まる。

【0 1 5 0】

次に、 $D'(1), D'(2)$ を取得して S を復元する場合には、次のようになる。

【0 1 5 1】

$$D'(1,1)*D'(2,1)=(S(1)*R(1)*R(2)*R'(1)*R'(2))*(S(1)*R(1)*R'(1))$$

$$=(S(1)*S(1))*(R(1)*R(1))*(R'(1)*R'(1))*R(2)*R'(2)$$

$$=0*0*0*R(2)*R'(2)$$

$$=R(2)*R'(2)$$

であるから、 $D'(1,1)*D'(2,1)$ を計算すれば、 $R(2)*R'(2)$ が求まる。

【0 1 5 2】

また同様に、

$$D'(1,2)*D'(2,2)=(S(2)*R(2)*R'(2))*(S(2)*R(1)*R(2)*R'(1)*R'(2))$$

$$=(S(2)*S(2))*R(1)*R'(1)*(R(2)*R(2))*(R'(2)*R'(2))$$

$$=0*R(1)*R'(1)*0*0$$

$$=R(1)*R'(1)$$

であるから、 $D'(1,2)*D'(2,2)$ を計算すれば、 $R(1)*R'(1)$ が求まる。

【0 1 5 3】

この $R(1)*R'(1), R(2)*R'(2)$ を使用して $S(1), S(2)$ を求める。

【0 1 5 4】

$$D'(2,1)*R(1)*R'(1)=(S(1)*R(1)*R'(1))*R(1)*R'(1)$$

$$=S(1)*(R(1)*R(1))*(R'(1)*R'(1))$$

$$=S(1)*0*0$$

$$=S(1)$$

であるから、 $D'(2,1)*R(1)*R'(1)$ を計算すれば、 $S(1)$ が求まる。

【0 1 5 5】

また同様に、

$$D'(1,2)*R(2)*R'(2)=(S(2)*R(2)*R'(2))*R(2)*R'(2)$$

$$=S(2)*(R(2)*R(2))*(R'(2)*R'(2))$$

$$=S(2)*0*0$$

$$=S(2)$$

であるから $D'(2,2)*R(2)*R'(2)$ を計算すれば $S(2)$ が求まる。

【0 1 5 6】

一般に、jを奇数として、

$$\begin{aligned} D'(1, j) * D'(2, j) &= (S(j) * R(j) * R(j+1) * R'(j) * R'(j+1)) * (S(j) * R(j) * R'(j)) \\ &= (S(j) * S(j)) * (R(j) * R(j)) * (R'(j) * R'(j)) * R(j+1) * R'(j+1) \\ &= 0 * 0 * 0 * R(j+1) * R'(j+1) \\ &= R(j+1) * R'(j+1) \end{aligned}$$

であるから $D'(1, j) * D'(2, j)$ を計算すれば $R(j+1) * R'(j+1)$ が求まる。

【0157】

また同様に、

$$\begin{aligned} D'(1, j+1) * D'(2, j+1) &= (S(j+1) * R(j+1) * R'(j+1)) * \\ &\quad (S(j+1) * R(j) * R(j+1) * R'(j) * R'(j+1)) \\ &= (S(j+1) * S(j+1)) * R(j) * R'(j) * \\ &\quad (R(j+1) * R(j+1)) * (R'(j+1) * R'(j+1)) \\ &= 0 * R(j) * R'(j) * 0 * 0 \\ &= R(j) * R'(j) \end{aligned}$$

であるから $D'(1, j+1) * D'(2, j+1)$ を計算すれば $R(j) * R'(j)$ が求まる。

【0158】

この $R(j) * R'(j)$, $R(j+1) * R'(j+1)$ を使用して $S(j)$, $S(j+1)$ を求める。

【0159】

$$\begin{aligned} D'(2, j) * R(j) * R'(j) &= (S(j) * R(j) * R'(j)) * R(j) * R'(j) \\ &= S(j) * (R(j) * R(j)) * (R'(j) * R'(j)) \\ &= S(j) * 0 * 0 \\ &= S(j) \end{aligned}$$

であるから $D'(2, j) * R(j) * R'(j)$ を計算すれば $S(j)$ が求まる。

【0160】

また同様に、

$$\begin{aligned} D'(1, j+1) * R(j+1) * R'(j+1) &= (S(j+1) * R(j+1) * R'(j+1)) * R(j+1) * R'(j+1) \\ &= S(j+1) * (R(j+1) * R(j+1)) * (R'(j+1) * R'(j+1)) \\ &= S(j+1) * 0 * 0 \\ &= S(j+1) \end{aligned}$$

であるから $D'(1, j+1) * R(j+1) * R'(j+1)$ を計算すれば $S(j+1)$ が求まる。

【0161】

以上、乱数追加注入方式により再分割データを生成した場合には、3つの再分割データ $D'(1)$, $D'(2)$, $D'(3)$ のすべてを用いなくても、3つの再分割データのうち、2つの再分割データを用いて上述したように元データを復元することができる。

【0162】

また、乱数追加注入方式においては、一旦元データを復元することなく（元データが見える形で現れない）、データの再分割処理を行うことができるので、よりセキュアなデータ管理が可能となる。

【0163】

（乱数書き換え方式）

図9は、乱数書き換え方式におけるデータ再分割処理の概要を説明するフローチャート図である。同図によれば、まず分割データ $D(1)$, $D(2)$, $D(3)$ を取得し（ステップS601）、次に、乱数発生部13で再分割の際に用いる乱数 R' を発生させる（ステップS603）。

【0164】

次に、分割データ $D(1)$, $D(2)$, $D(3)$ それぞれに乱数 R' を上述した乱数追加注入方式により注入する（ステップS605）。次に、乱数 R' を注入された分割データから旧乱数である R を消去して、新たな再分割データ $D'(1)$, $D'(2)$, $D'(3)$ を生成する（ステップS607, S609）。

【0165】

図10は、元データSを、元データの半分の長さの処理単位ビット長bに基づいて分割数 $n=3$ で3分割する場合の分割部分データの定義式、乱数 R' の再注入後の分割部分データの定義式、さらに乱数Rを消去後の分割部分データの定義式および各分割部分データから元データを復元する場合の計算式などを示す表である。

【0166】

本方式においては、ステップS605までは、上述した乱数追加注入方式と同様であるため、説明は省略し、古い乱数Rを消去した分割部分データの定義式について説明する。

【0167】

まず、第1の分割データ $D'(1)$ に対しては、図10に示すように、第1の分割部分データ $D'(1,1)$ は、定義式 $(S(1)*R(1)*R(2)*R'(1)*R'(2))*(R(1)*R(2))$ 、即ち、 $S(1)*R'(1)*R'(2)$ で定義され、第2の分割部分データ $D'(1,2)$ は、定義式 $(S(2)*R(2)*R'(2))*R(2)$ 、即ち、 $S(2)*R'(2)$ で定義される。なお、この定義式の一般形は、 $D'(1,j)$ に対しては $S(j)*R'(j)*R'(j+1)$ であり、 $D'(1,j+1)$ に対して $S(j+1)*R'(j+1)$ である(j は奇数とする)。

【0168】

また、第2の分割データ $D'(2)$ に対しては、図10に示すように、 $D'(2,1)$ は $(S(1)*R(1)*R'(1))*R(1)$ 、即ち、 $S(1)*R'(1)$ で定義され、 $D'(2,2)$ は $(S(2)*R(1)*R(2)*R'(1)*R'(2))*R(1)*R(2)$ 、即ち、 $S(2)*R'(1)*R'(2)$ で定義される。この定義式の一般形は、 $D'(2,j)$ に対しては $S(j)*R'(j)*R'(j+1)$ であり、 $D(2,j+1)$ に対しては $S(j+1)*R'(j)*R'(j+1)$ である(j は奇数とする)。

【0169】

また、第3の分割データ $D'(3)$ に対しては、図10に示すように、 $D'(3,1)$ は $(R(1)*R'(1))*R(1)$ 、即ち、 $R'(1)$ で定義され、 $D'(3,2)$ は $(R(2)*R'(2))*R(2)$ 、即ち、 $R'(2)$ で定義される。この定義式の一般形は、 $D'(3,j)$ に対しては $R'(j)*R'(j+1)$ であり、 $D(3,j+1)$ に対しては $R'(j+1)$ である(j は奇数とする)。

【0170】

このように、再分割部分データ $D'(i,j)$ はそれぞれ、分割部分データ $D(i,j)$ に、分割部分データ $D(i,j)$ の定義式で注入されていた乱数部分データ $R(j)$ に対応する乱数部分データ $R'(j)$ を注入した後、さらに乱数部分データ $R(j)$ を消去するように乱数部分データ $R(j)$ を注入して排他的論理和を計算し、求めるものである。

【0171】

その結果、もとの分割部分データ $D(i,j)$ の定義式において、乱数部分データ $R(j)$ を乱数部分データ $R'(j)$ に置換したものが、再分割部分データ $D'(i,j)$ の定義式となる。

【0172】

次に、図10の右側に示す表を参照して、再分割データから元データを復元する処理について説明する。これは、ユーザが再分割データを受け取った後のサービス利用時において、機密情報管理システム1の元データ復元部12の機能を説明するものである。

【0173】

まず、分割部分データ $D'(2,1), D'(3,1)$ から第1の元部分データ $S(1)$ を次のように生成することができる。

【0174】

$$\begin{aligned} D'(2,1)*D'(3,1) &= (S(1)*R'(1))*R'(1) \\ &= S(1)*(R'(1)*R'(1)) \\ &= S(1)*0 \\ &= S(1) \end{aligned}$$

また、別の分割部分データから次のように第2の元部分データ $S(2)$ を生成することができる。

【0175】

$$\begin{aligned} D'(2,2)*D'(3,1)*D'(3,2) &= (S(2)*R'(1)*R'(2))*R'(1)*R'(2) \\ &= S(2)*(R'(1)*R'(1))*(R'(2)*R'(2)) \end{aligned}$$

$$=S(2)*0*0$$

$$=S(2)$$

一般に、jを奇数として、

$$D'(2,j)*D'(3,j)=(S(j)*R'(j))*R'(j)$$

$$=S(j)*(R'(j)*R'(j))$$

$$=S(j)*0$$

$$=S(j)$$

であるから、 $D'(2,j)*D'(3,j)$ を計算すれば、 $S(j)$ が求まる。

【0 1 7 6】

また、一般に、jを奇数として、

$$D'(2,j+1)*D'(3,j)*D'(3,j+1)=(S(j+1)*R'(j)*R'(j+1))*R'(j)*R'(j+1)$$

$$=S(j+1)*(R'(j)*R'(j))*(R'(j+1)*R'(j+1))$$

$$=S(j+1)*0*0$$

$$=S(j+1)$$

であるから、 $D'(2,j+1)*D'(3,j)*D'(3,j+1)$ を計算すれば、 $S(j+1)$ が求まる。

【0 1 7 7】

次に、 $D'(1), D'(3)$ を取得してSを復元する場合には、次のようになる。

【0 1 7 8】

$$D'(1,1)*D'(3,1)*D'(3,2)=(S(1)*R'(1)*R'(2))*R'(1)*R'(2)$$

$$=S(1)*(R'(1)*R'(1))*(R'(2)*R'(2))$$

$$=S(1)*0*0$$

$$=S(1)$$

であるから、 $D'(1,1)*D'(3,1)*D'(3,2)$ を計算すれば、 $S(1)$ が求まる。

【0 1 7 9】

また同様に、

$$D'(1,2)*D'(3,2)=(S(2)*R'(2))*R'(2)$$

$$=S(2)*(R'(2)*R'(2))$$

$$=S(2)*0$$

$$=S(2)$$

であるから、 $D'(1,2)*D'(3,2)$ を計算すれば、 $S(2)$ が求まる。

【0 1 8 0】

一般に、jを奇数として、

$$D'(1,j)*D'(3,j)*D'(3,j+1)=(S(j)*R'(j)*R'(j+1))*R'(j)*R'(j+1)$$

$$=S(j)*(R'(j)*R'(j))*(R'(j+1)*R'(j+1))$$

$$=S(j)*0*0$$

$$=S(j)$$

であるから、 $D'(1,j)*D'(3,j)*D'(3,j+1)$ を計算すれば、 $S(j)$ が求まる。

【0 1 8 1】

また、一般に、jを奇数として、

$$D'(1,j+1)*D'(3,j+1)=(S(j+1)*R'(j+1))*R'(j+1)$$

$$=S(j+1)*(R'(j+1)*R'(j+1))$$

$$=S(j+1)*0$$

$$=S(j+1)$$

であるから、 $D'(1,j+1)*D'(3,j+1)$ を計算すれば、 $S(j+1)$ が求まる。

【0 1 8 2】

次に、 $D'(1), D'(2)$ を取得してSを復元する場合には、次のようになる。

【0 1 8 3】

$$D'(1,1)*D'(2,1)=(S(1)*R'(1)*R'(2))*(S(1)*R'(1))$$

$$=(S(1)*S(1))*(R'(1)*R'(1))*R'(2)$$

$$=0*0*R'(2)$$

$$= R' (2)$$

であるから、 $D' (1, 1) * D' (2, 1)$ を計算すれば、 $R' (2)$ が求まる。

【0 1 8 4】

また同様に、

$$\begin{aligned} D' (1, 2) * D' (2, 2) &= (S(2) * R' (2)) * (S(2) * R' (1) * R' (2)) \\ &= (S(2) * S(2)) * (R' (2) * R' (2)) * R' (1) \\ &= 0 * 0 * R' (1) \\ &= R' (1) \end{aligned}$$

であるから、 $D' (1, 2) * D' (2, 2)$ を計算すれば、 $R' (1)$ が求まる。

【0 1 8 5】

この $R' (1)$, $R' (2)$ を使用して $S(1)$, $S(2)$ を求める。

【0 1 8 6】

$$\begin{aligned} D' (2, 1) * R' (1) &= (S(1) * R' (1)) * R' (1) \\ &= S(1) * (R' (1) * R' (1)) \\ &= S(1) * 0 \\ &= S(1) \end{aligned}$$

であるから、 $D' (2, 1) * R' (1)$ を計算すれば、 $S(1)$ が求まる。

【0 1 8 7】

また同様に、

$$\begin{aligned} D' (1, 2) * R' (2) &= (S(2) * R' (2)) * R' (2) \\ &= S(2) * (R' (2) * R' (2)) \\ &= S(2) * 0 \\ &= S(2) \end{aligned}$$

であるから $D' (1, 2) * R' (2)$ を計算すれば $S(2)$ が求まる。

【0 1 8 8】

一般に、 j を奇数として、

$$\begin{aligned} D' (1, j) * D' (2, j) &= (S(j) * R' (j) * R' (j+1)) * (S(j) * R' (j)) \\ &= (S(j) * S(j)) * (R' (j) * R' (j)) * R' (j+1) \\ &= 0 * 0 * R' (j+1) \\ &= R' (j+1) \end{aligned}$$

であるから $D' (1, j) * D' (2, j)$ を計算すれば $R' (j+1)$ が求まる。

【0 1 8 9】

また同様に、

$$\begin{aligned} D' (1, j+1) * D' (2, j+1) &= (S(j+1) * R' (j+1)) * (S(j+1) * R' (j) * R' (j+1)) \\ &= (S(j+1) * S(j+1)) * (R' (j+1) * R' (j+1)) * R' (j) \\ &= 0 * 0 * R' (j) \\ &= R' (j) \end{aligned}$$

であるから $D' (1, j+1) * D' (2, j+1)$ を計算すれば $R' (j)$ が求まる。

【0 1 9 0】

この $R' (j)$, $R' (j+1)$ を使用して $S(j)$, $S(j+1)$ を求める。

【0 1 9 1】

$$\begin{aligned} D' (2, j) * R' (j) &= (S(j) * R' (j)) * R' (j) \\ &= S(j) * (R' (j) * R' (j)) \\ &= S(j) * 0 \\ &= S(j) \end{aligned}$$

であるから $D' (2, j) * R' (j)$ を計算すれば $S(j)$ が求まる。

【0 1 9 2】

また同様に、

$$\begin{aligned} D' (1, j+1) * R' (j+1) &= (S(j+1) * R' (j+1)) * R' (j+1) \\ &= S(j+1) * (R' (j+1) * R' (j+1)) \end{aligned}$$

$$\begin{aligned} &=S(j+1)*0 \\ &=S(j+1) \end{aligned}$$

であるから $D'(1, j+1) * R'(j+1)$ を計算すれば $S(j+1)$ が求まる。

【0193】

以上、乱数書き換え方式により再分割データを生成した場合には、3つの再分割データ $D'(1), D'(2), D'(3)$ のすべてを用いなくても、3つの再分割データのうち、2つの再分割データを用いて上述したように元データを復元することができる。

【0194】

また、乱数書き換え方式においても、一旦元データを復元することなく（元データが見える形で現れない）、データの再分割処理を行うことができるので、よりセキュアなデータ管理が可能となる。

【0195】

<動作>

次に、本実施の形態に係る機密情報管理システム1が適用されるコンピュータシステム10全体の動作について説明する。ここで、図11は、ユーザが機密情報Sを機密情報管理システム1に登録する動作を説明するシーケンス図であり、図12は、ユーザがサービスを利用する時の機密情報管理システム1の動作を説明するシーケンス図であり、図13は、ユーザが保持する分割データDを紛失したときの機密情報管理システム1の動作を説明するシーケンス図である。

【0196】

(1) 機密情報登録処理

まず、ユーザが端末2から通信ネットワーク4を介して機密情報管理システム1に機密情報Sを送信する（ステップS10）。機密情報システム1は、機密情報Sを受け取ると、上述した秘密分散法Aを用いて3つのデータ（分割データ） $D(1), D(2), D(3)$ に分割する（ステップS20）。

【0197】

次に、機密情報管理システム1は、このようにして生成された分割データを各保管サーバ3a, 3bおよび端末2にネットワーク4を介して送信する（ステップS30）。

【0198】

次に、保管サーバ3a, 3bは、それぞれ送信されてきた分割データ $D(1), D(2)$ をハードディスク等の記憶装置に記憶する（ステップS40）。また、端末2は、送信されてきた分割データ $D(3)$ をハードディスク等の記憶装置に記憶する（ステップS50）。

【0199】

これにより、端末2、保管サーバ3a, 3bのうちいずれか1つの分割データに紛失、破壊等があっても、残りの2つの分割データからもとの機密情報Sを復元できる。

【0200】

(2) サービス利用処理

ユーザがサービス提供システム5を利用する場合には、まず、端末2に保持する分割データ $D(3)$ を通信ネットワークを介して機密情報管理システム1に送信する（ステップS110）。

【0201】

機密情報管理システム1は、端末2から分割データ $D(3)$ を受け取ると、残りの分割データ $D(1), D(2)$ を保管サーバ3a, 3bに要求し、該分割データ $D(1), D(2)$ を受け取る（ステップS120）。

【0202】

次に、機密情報管理システム1は、分割データ $D(1), D(2), D(3)$ のいずれか2つから秘密分散法Aを用いて機密情報Sを復元する（ステップS130）。そして、復元した機密情報Sをサービス提供5に送信して（ステップS140）、機密情報Sを復元し送信した事実を使用履歴として生成する（ステップS150）。

【0203】

サービス提供システム 5 は、機密情報管理システム 1 から機密情報 S を受け取ると、該機密情報 S の正当性を判断して、端末 2 に通信ネットワーク 4 を介してサービス提供を行う（ステップ S 160, S 170）。これにより、ユーザは所望のサービスの提供を受けることができる。

【0204】

(3) 分割データ紛失時処理

ユーザが分割データ D(3) を紛失した場合（例えば、分割データ D(3) を記憶している端末 2 を紛失した場合）には、まず、機密情報管理システム 1 にその旨を申告する（例えば、機密情報管理システム 1 の運用者へ電話連絡する）（ステップ S 210）。

【0205】

これにより、機密情報管理システム 1 は、保管サーバ 3 a, 3 b に分割データを要求し、保管サーバ 3 a, 3 b からそれぞれ分割データ D(1), D(2) を受け取る（ステップ S 220）。

【0206】

次に、機密情報管理システム 1 は、分割データ D(1), D(2) から秘密分散法 A を用いて、新たに 3 つのデータ（再分割データ）D' (1), D' (2), D' (3) を生成する（ステップ S 240）。

【0207】

ここで、再分割データ D' (1), D' (2) に関しては、上述した乱数追加注入方式又は乱数書き換え方式に従って、分割データ D(1), D(2) からそれぞれ生成するものである。一方、D' (3) は、まず、分割データ D (1), D (2) から分割データ D (3) を生成し、その後、乱数追加注入方式又は乱数書き換え方式に従って、分割データ D (3) から D' (3) を生成するものである。

【0208】

次に、機密情報管理システム 1 は、このようにして生成された再分割データを各保管サーバ 3 a, 3 b および端末 2（例えば、ユーザが分割データ D(3) を記憶している端末 2 を紛失した場合には、ユーザが新たに購入した端末 2）にネットワーク 4 を介して送信する（ステップ S 250, S 260）。

【0209】

次に、保管サーバ 3 a, 3 b は、それぞれ送信されてきた再分割データ D' (1), D' (2) をハードディスク等の記憶装置に記憶する（ステップ S 250）。また、端末 2 は、送信されてきた分割データ D' (3) をハードディスク等の記憶装置に記憶する（ステップ S 260）。これにより、ユーザは再びサービス利用が可能となる。

【0210】

従って、本実施の形態によれば、所定のサービスを受ける際に必要とされる機密情報 S を秘密分散法 A を用いて複数に分割して、そのうちの一部をユーザに保持させるので、ユーザが保持する分割データの紛失があったとしても、残りの分割データから機密情報 S を復元できるとともに、秘密分散法 A を用いて新たに再分割データを生成し、該再分割データの一部を新たにユーザに保持させるので、機密情報 S の変更は不要である。

【0211】

この結果、ユーザが保持する分割データの紛失があったとしても、機密情報 S の再発行処理をすることなく、紛失の申告をするだけで、再びサービス提供を受けることができる。

【0212】

特に、本発明における秘密分散法は、機密情報を所望の処理単位ビット長に基づいて所望の分割数の分割データに分割するデータ分割方法であり、機密情報を処理単位ビット長毎に区分けして、複数の元部分データを生成し、この複数の元部分データの各々に対応して、機密情報のビット長と同じまたはこれより短い長さの乱数から処理単位ビット長の複数の乱数部分データを生成し、各分割データを構成する各分割部分データを元部分データと乱数部分データの排他的論理和によって処理単位ビット長毎に生成して、所望の分割数



の分割データを生成するとともに、生成した分割データのうちの所定の個数の分割データから機密情報が復元することができ、また、新たに発生させた乱数から処理単位ビット長の複数の乱数部分データを生成し、各分割部分データと該乱数部分データの排他的論理和により処理単位ビット長毎に再分割部分データを生成して、所望の分割数の再分割データを生成するとともに、生成した再分割データのうちの所定の個数の再分割データから機密情報が復元することができるので、機密情報を復元することなく、機密情報を再分割することができる。

【0213】

これにより、ユーザの機密情報をよりセキュアに管理することができる。

また、紛失した分割データを取得した第3者が機密情報管理システム1にアクセスしても機密情報Sを復元することができないので、サービスを利用することができず、安全性が確保される。

【0214】

さらに、ユーザの使用履歴が機密情報管理システム1に保管されるので、ユーザが分割データを紛失してから紛失した旨を申告するまでの間に、仮に第3者が機密情報Sを取得して悪用したとしても、使用履歴により悪用の有無を判別することができる。

【0215】

尚、本実施の形態における秘密分散法Aは、多項式演算・剰余演算などを含む多倍長整数の演算処理を必要としないので、大容量データを多数処理する場合においても簡単かつ迅速にデータの分割および復元を行うことができるという効果を得ることができる。

【0216】

以上、本発明の実施の形態について説明してきたが、本発明の要旨を逸脱しない範囲において、本発明の実施の形態に対して種々の変形や変更を施すことができる。例えば、上記実施の形態においては、端末2から機密情報Sの機密情報管理システム1への受け渡しを通信ネットワーク4を介して行ったが、本発明はこれに限定されず、例えば、機密情報Sを記録した記録媒体を郵送など通信ネットワーク3以外の手段を介して受け渡してもよい。また、同様に、ユーザが保持する分割データも通信ネットワーク4を介して受け取ったが、本発明はこれに限定されず、例えば、分割データを記録した記録媒体を郵送など通信ネットワーク3以外の手段を介して受け渡してもよい。

【0217】

また、上記実施の形態においては、ユーザがサービス利用時には、機密情報管理システム1が機密情報を復元したが、本発明はこれに限定されず、ユーザの端末2が、端末2に記憶される分割データと機密情報管理システム1から取得した分割データから、秘密分散法Aを用いて機密情報を復元し、該機密情報をサービス提供システム5に送信してもよいものである。尚、この場合には、復元された機密情報が端末2に記憶されたままユーザが端末2を紛失すると、本発明が解決しようとする課題が解決できないことになるため、該機密情報をサービス提供システム5に送信後すぐに端末2から消去する仕組み、あるいは、端末2のデータの第三者による不正な取り出しを防止する仕組みなどを備えることが必要である。

【0218】

さらに、上記実施の形態においては、ユーザからの要求により再分割処理を行ったが、機密情報管理システム1が自発的に所定の契機により再分割処理を行ってもよいものである。

【図面の簡単な説明】

【0219】

【図1】本発明の実施の形態に係る機密情報管理システムが適用されるコンピュータシステム全体の概略構成を示すブロック図である。

【図2】本発明の実施の形態に係る機密情報管理システムの分割数 $n=3$ の場合の分割処理を示すフローチャートである。

【図3】16ビットの元データSを8ビットの処理単位ビット長に基づいて分割数 $n=3$

で3分割する場合の各データと定義式および各分割部分データから元データを復元する場合の計算式などを示す表である。

【図4】分割数 $n=3$ の場合の分割データ、分割部分データ、各分割部分データを生成する定義式を示す表である。

【図5】本発明の実施の形態に係る機密情報管理システムの分割数が n で処理単位ビット長が b である場合の一般的な分割処理を示すフローチャートである。

【図6】分割数 $n=3$ の場合の分割データ、分割部分データ、各分割部分データを生成する定義式の別の例を示す表である。

【図7】本発明の実施の形態に係る機密情報管理システムにおけるデータ再分割処理(乱数追加注入方式)を示すフローチャートである。

【図8】乱数追加注入方式により元データ S を元データ S の半分の長さの処理単位ビット長に基づいて分割数 $n=3$ で再分割する場合の各データと定義式および各分割部分データから元データを復元する場合の計算式などを示す表である。

【図9】本発明の実施の形態に係る機密情報管理システムにおけるデータ再分割処理(乱数書き換え方式)を示すフローチャートである。

【図10】乱数書き換え方式により元データ S を元データ S の半分の長さの処理単位ビット長に基づいて分割数 $n=3$ で再分割する場合の各データと定義式および各分割部分データから元データを復元する場合の計算式などを示す表である。

【図11】本発明の実施の形態に係る機密情報管理システムにおいて機密情報を登録する処理を説明するシーケンス図である。

【図12】本発明の実施の形態に係る機密情報管理システムにおいてサービス利用時の処理を説明するシーケンス図である。

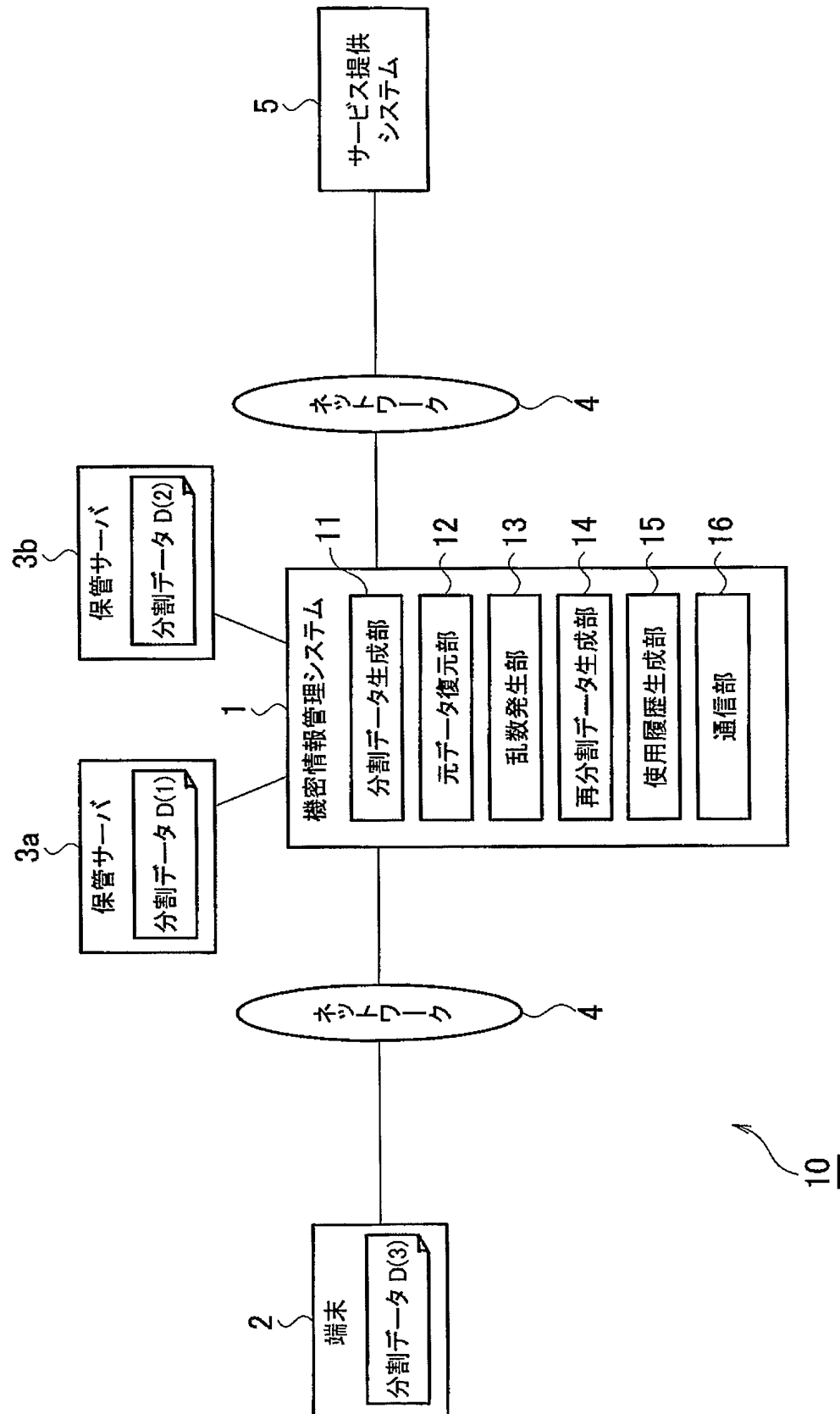
【図13】本発明の実施の形態に係る機密情報管理システムにおいてユーザが保持する機密情報の一部を紛失したときの処理を説明するシーケンス図である。

【符号の説明】

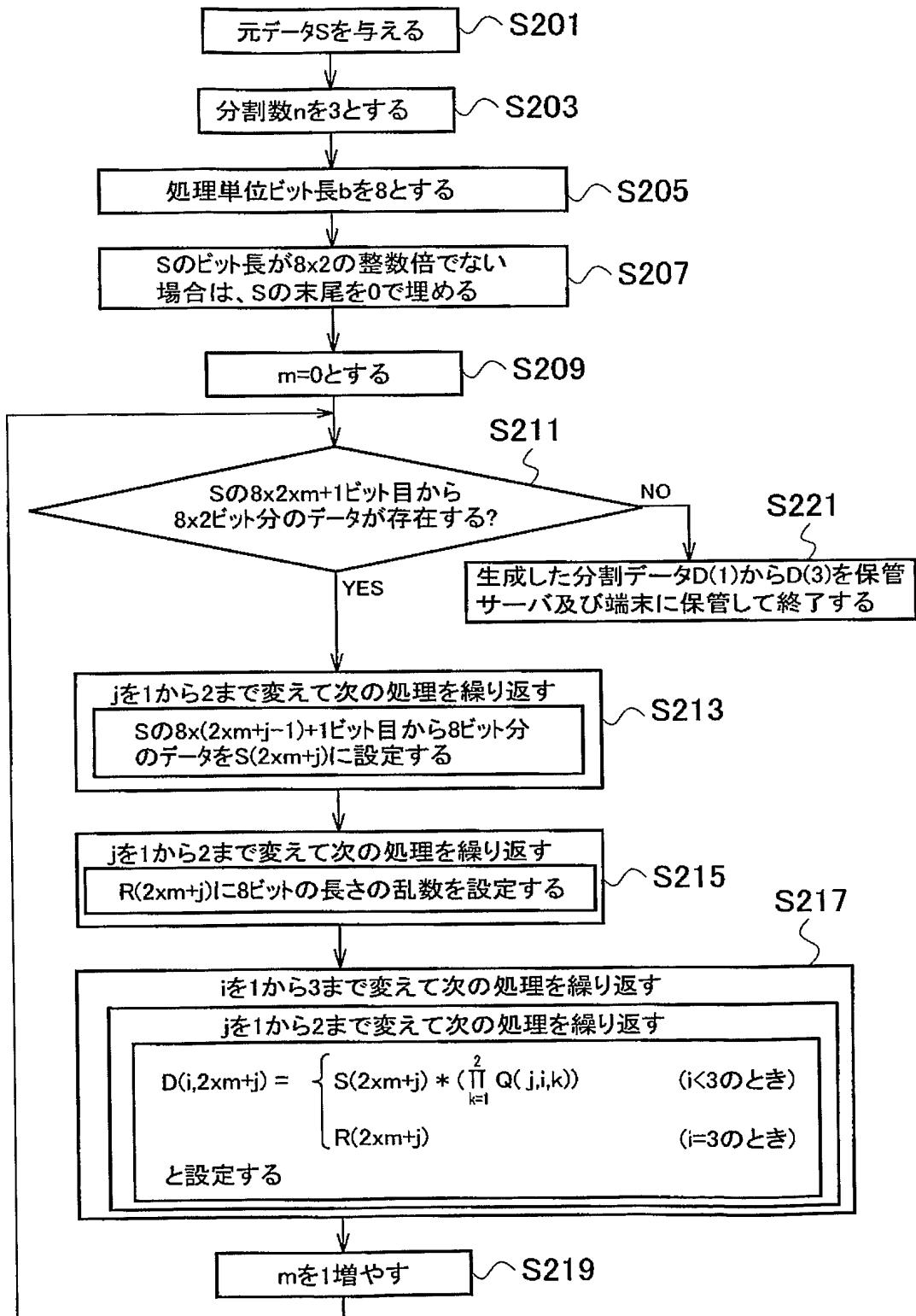
【0220】

- 1…機密情報管理システム
- 2…端末
- 3 a, 3 b…保管サーバ
- 4…通信ネットワーク
- 5…サービス提供システム
- 10…コンピュータシステム
- 11…分割データ生成部
- 12…元データ復元部
- 13…乱数発生部
- 14…再分割データ生成部
- 15…使用履歴生成部
- 16…通信部

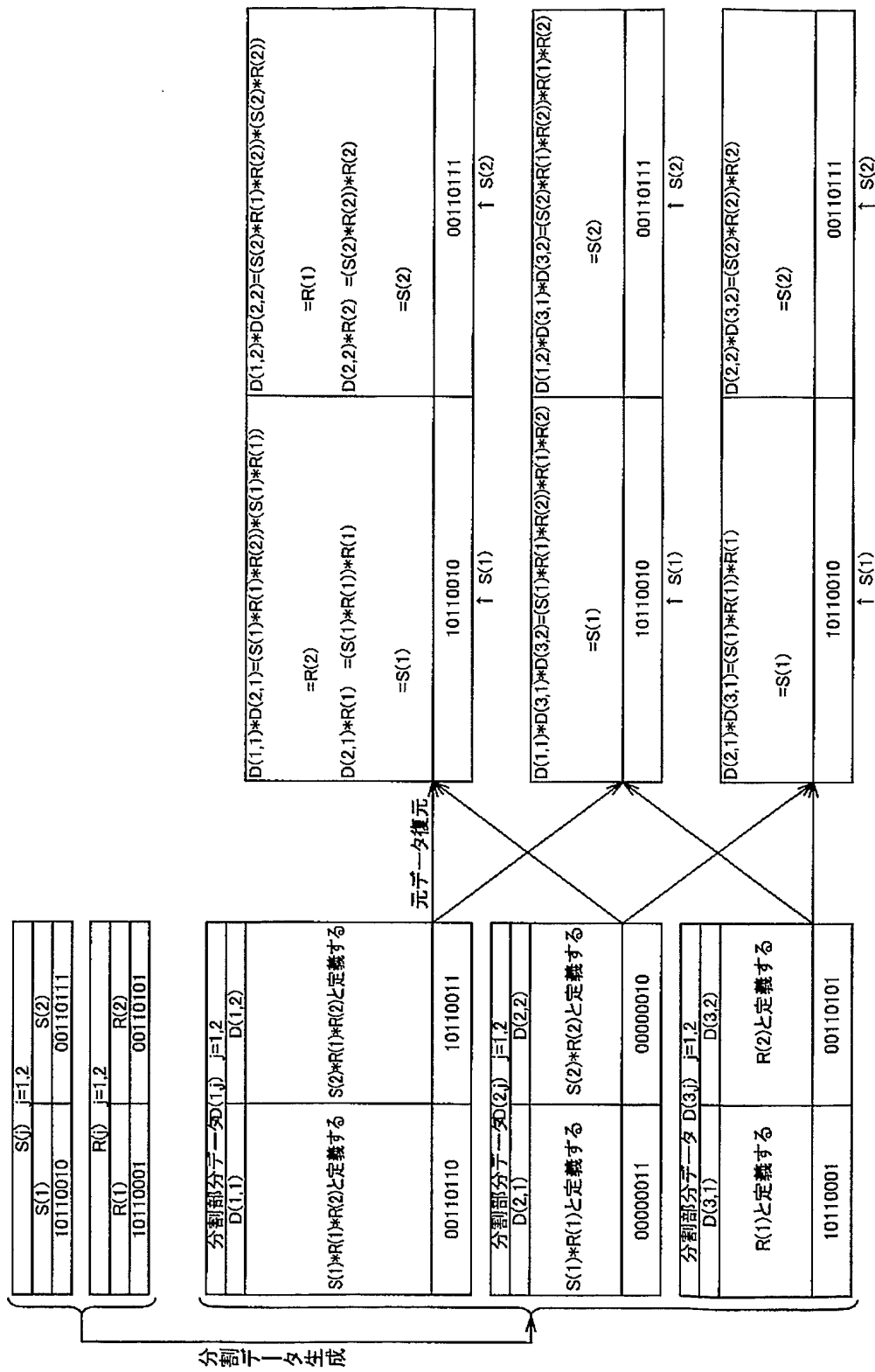
【書類名】 図面
【図 1】



【図 2】



【図 3】



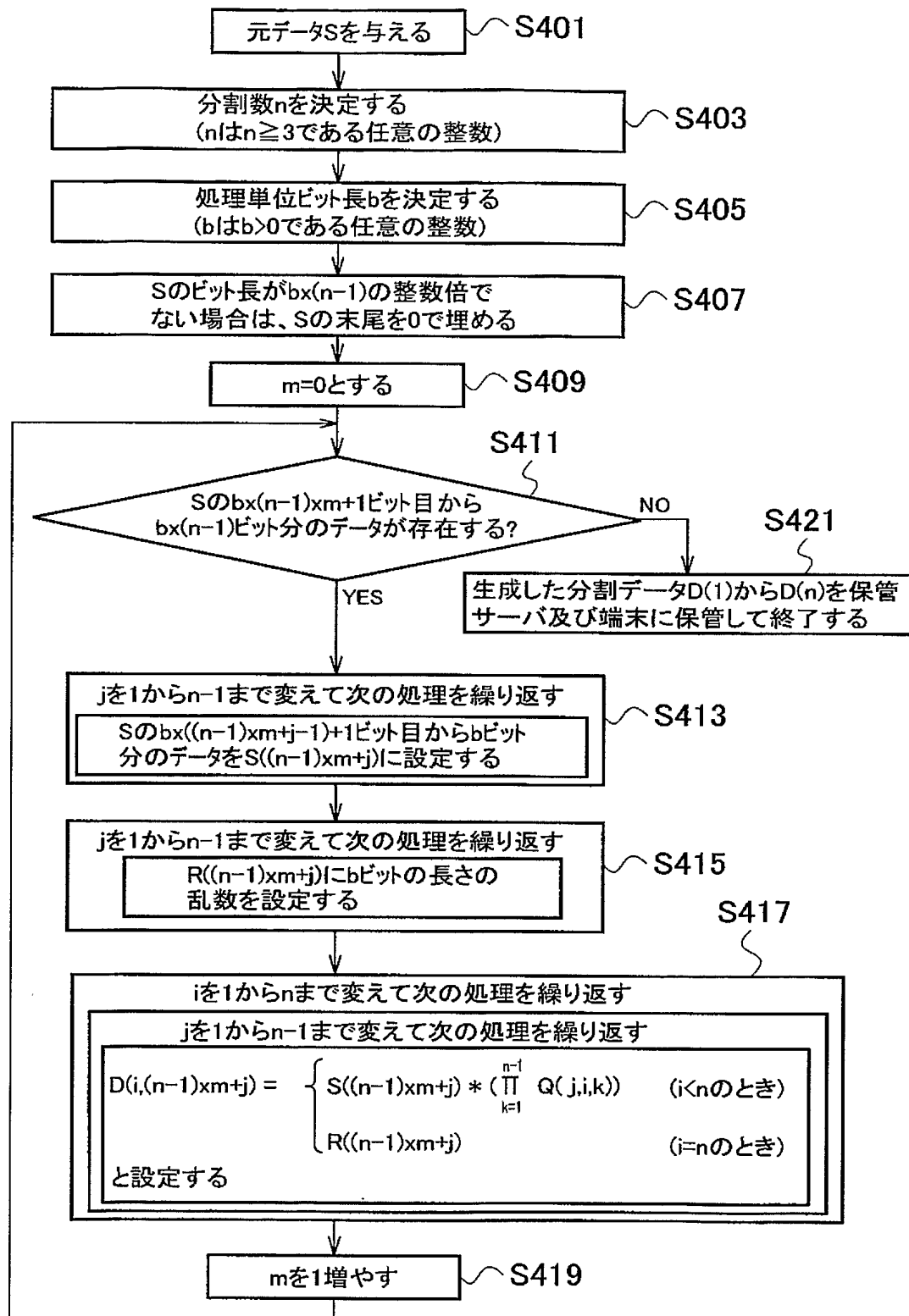


【図 4】

3分割 ($n=3$)
任意の2つの分割データから元データが復元可能。

jの値		1	2	...	$j=2 \times m+1$	$j+1$	→元データSの末尾まで続く
元データ S(j)		S(1)	S(2)	...	S(j)	S(j+1)	...
乱数 R(j)		R(1)	R(2)	...	R(j)	R(j+1)	...
分割部分データD(1,j)		$S(1)*R(1)*R(2)$	$S(2)*R(1)*R(2)$...	$S(j)*R(j)*R(j+1)$	$S(j+1)*R(j)*R(j+1)$...
分割部分データD(2,j)		$S(1)*R(1)$	$S(2)*R(2)$...	$S(j)*R(j)$	$S(j+1)*R(j+1)$...
分割部分データD(3,j)		R(1)	R(2)	...	R(j)	R(j+1)	...

【図 5】

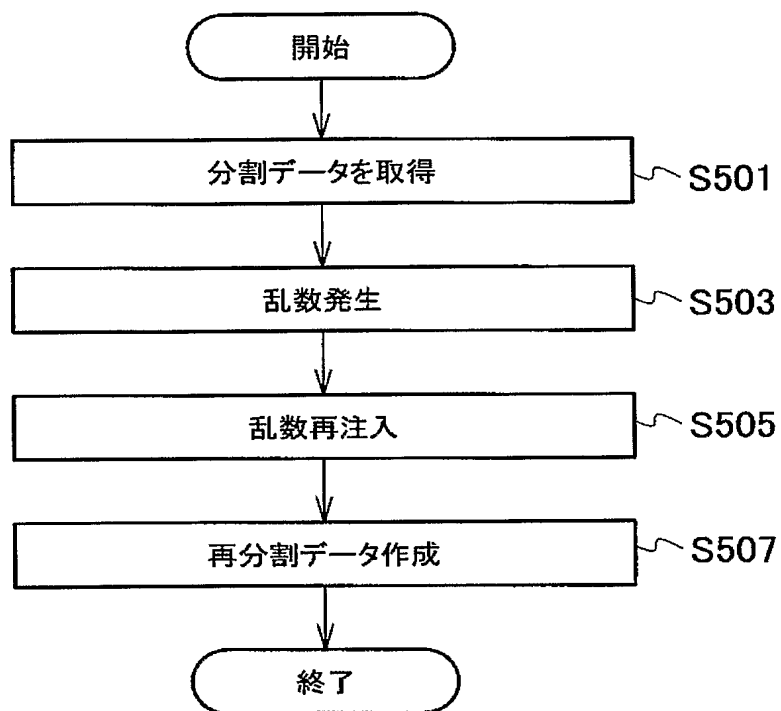


【図 6】

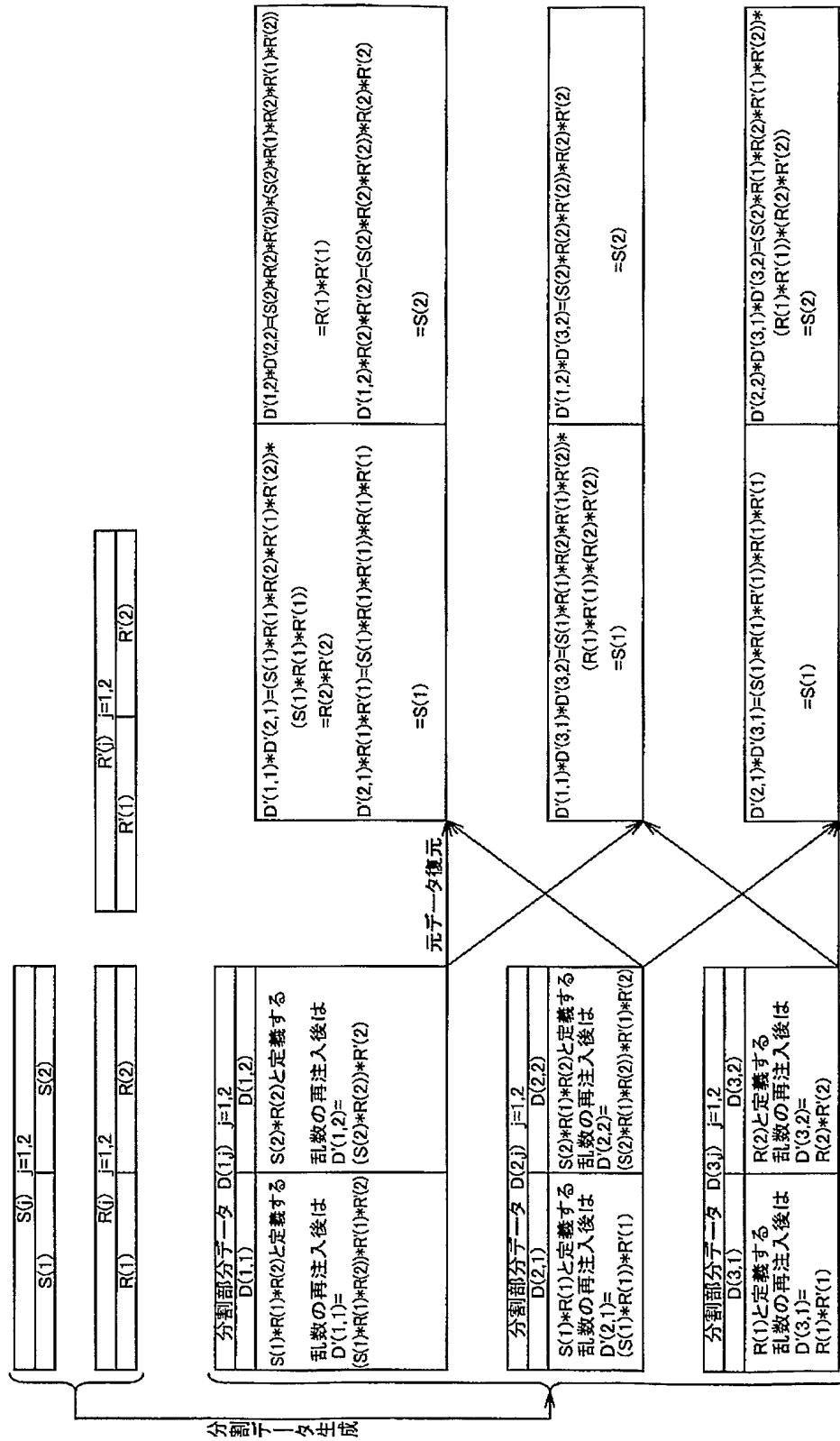
3分割 (n=3)
任意の2つの分割データから元データが復元可能。

		(mはm>0の任意の整数)				→元データSの末尾まで続く	
jの値	1	2	...	j=2×m+1	j+1		...
元データ S(j)	S(1)	S(2)	...	S(j)	S(j+1)		...
乱数 R(j)	R(1)	R(2)	...	R(j)	R(j+1)		...
分割データD(1,j)	S(1)*R(1)*R(2)	S(2) *R(2)	...	S(j)*R(j)*R(j+1)	S(j+1) *R(j+1)		...
分割データD(2,j)	S(1)*R(1)	S(2)*R(1)*R(2)	...	S(j)*R(j)	S(j+1)*R(j)*R(j+1)		...
分割データD(3,j)	R(1)	R(2)	...	R(j)	R(j+1)		...

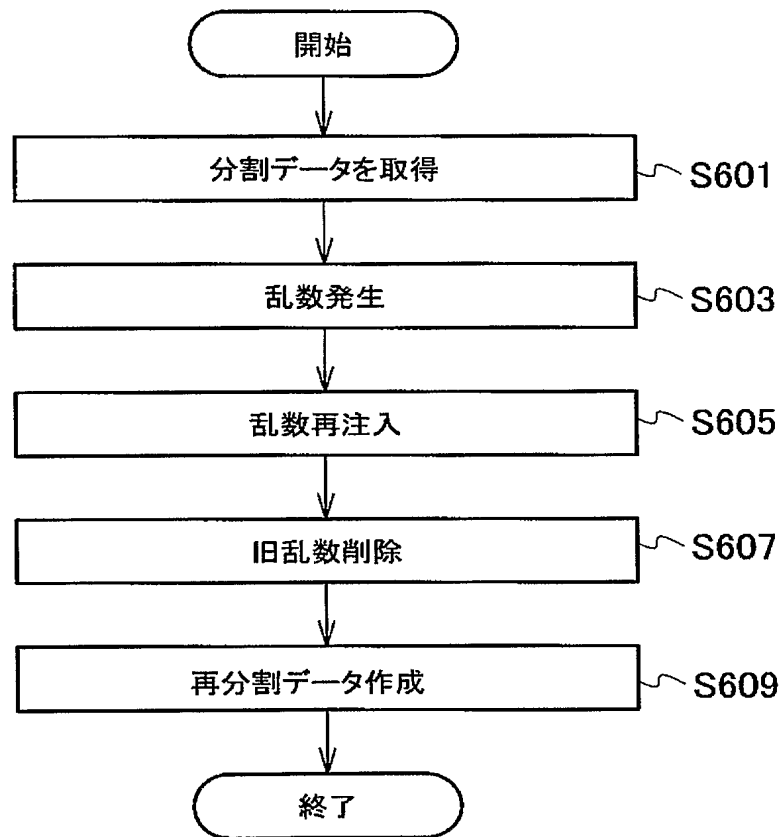
【図 7】



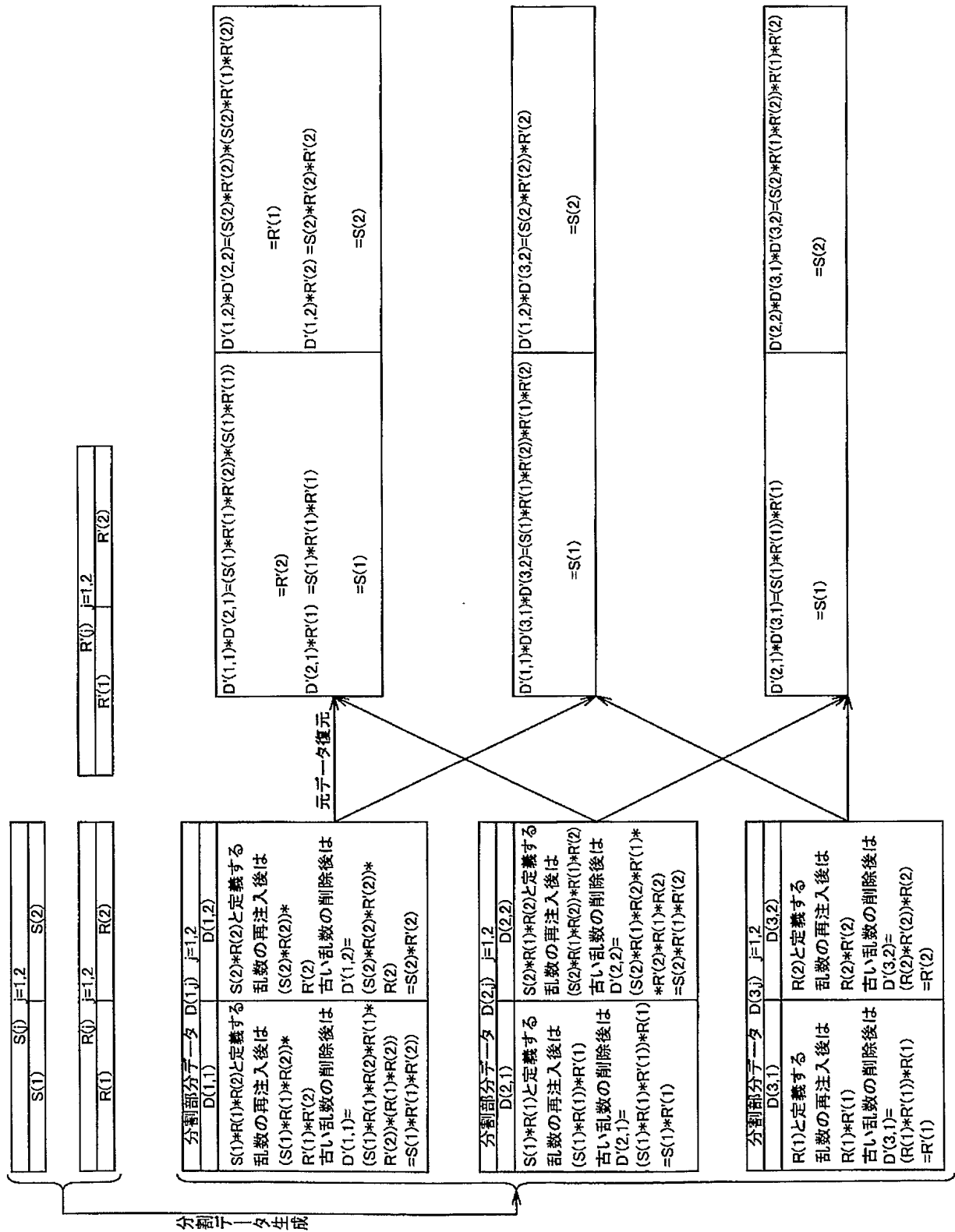
【図 8】



【図 9】

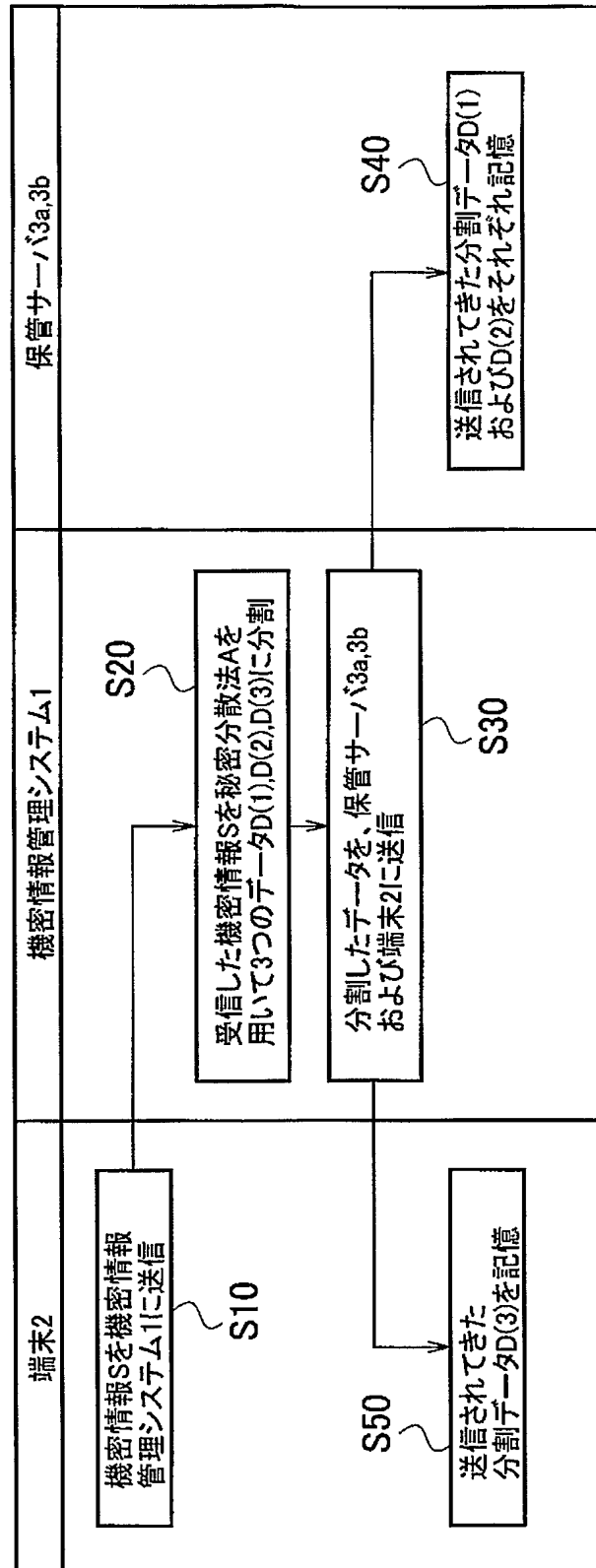


【図 10】



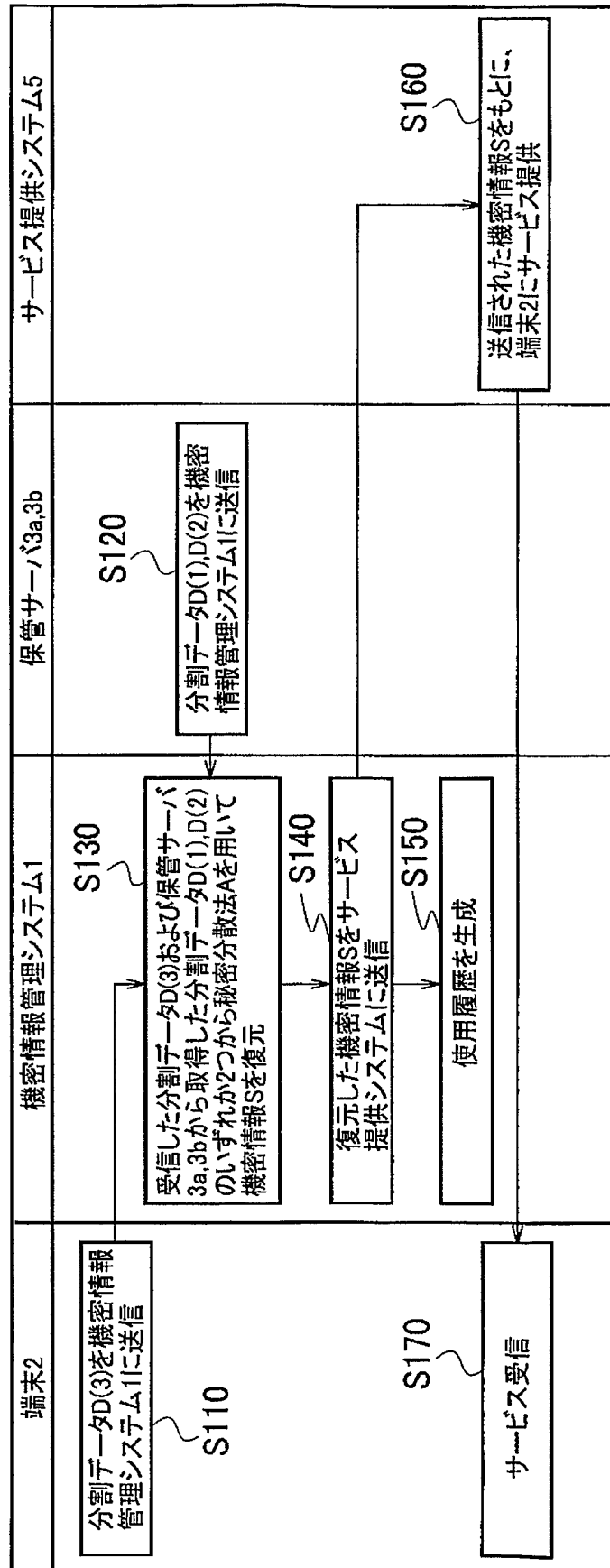


【図 11】



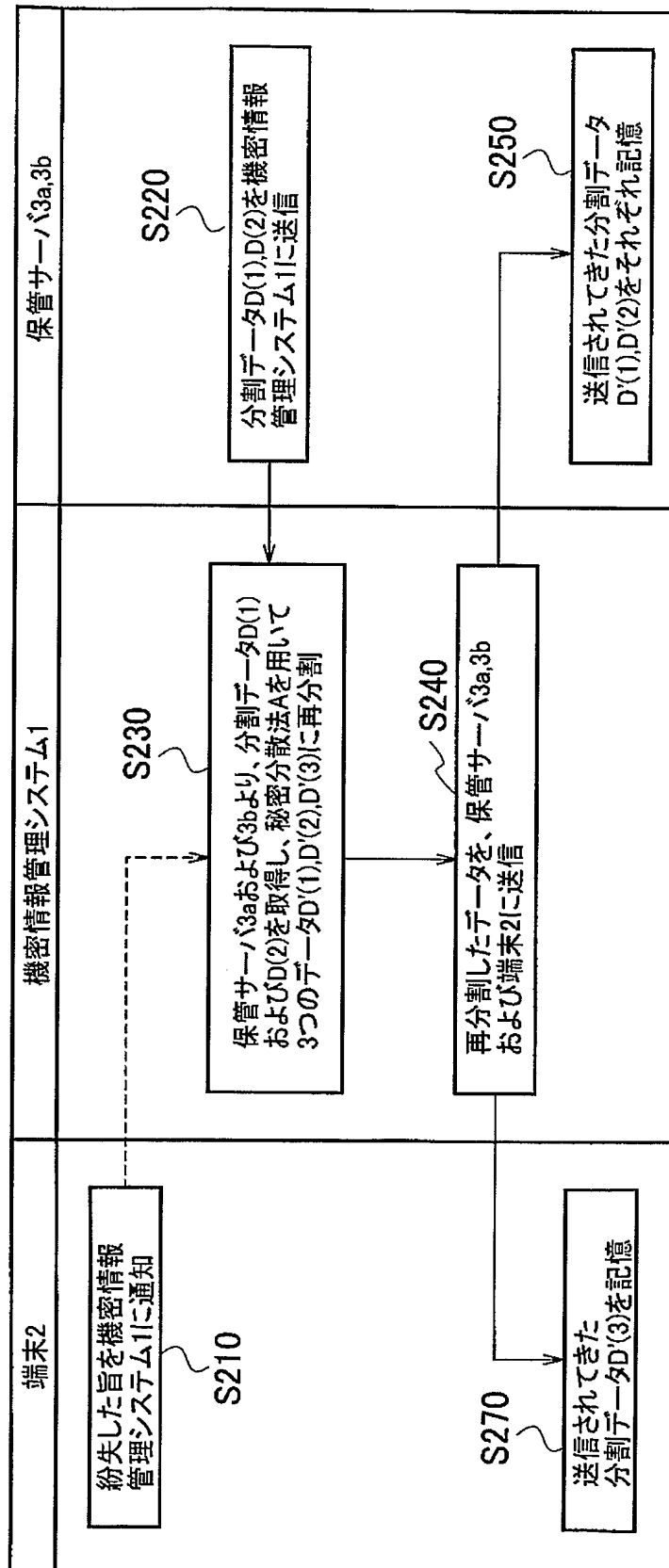


【図 12】





【図 13】



【書類名】 要約書

【要約】

【課題】 ユーザが保持するサービス利用のための情報を紛失しても、機密情報を変更することなくサービスの提供を受けることができる。

【解決手段】 端末 2 が機密情報 S を機密情報管理システム 1 に送信すると、機密情報管理システム 1 は、秘密分散法 A を用いて機密情報 S を複数のデータに分割し、分割データを保管サーバ 3 a, 3 b 及び端末 2 に保管させる。サービス利用時は、端末 2 から分割データを機密情報管理システム 1 に送信すると、機密情報管理システム 1 は、該分割データおよび保管サーバ 3 a, 3 b の分割データから秘密分散法 A を用いて機密情報 S を復元し、機密情報 S をサービス提供システム 5 に送信する。ユーザが分割データを紛失した際は、機密情報管理システム 1 は、保管サーバ 3 a, 3 b の分割データから秘密分散法 A を用いて再分割データを生成し、保管サーバ 3 a, 3 b 及び端末 2 に保管させる。

【選択図】 図 1



特願 2 0 0 4 - 0 3 3 3 5 2

出 願 人 履 歴 情 報

識別番号

[3 9 9 0 3 5 7 6 6]

1. 変更年月日

1 9 9 9 年 6 月 9 日

[変更理由]

新規登録

住 所

東京都千代田区内幸町一丁目 1 番 6 号

氏 名

エヌ・ティ・ティ・コミュニケーションズ株式会社